MailFoundry User Manual
Revision: MF20120621
Copyright © 2007, Solinus Inc. – All Rights Reserved

Table of Contents

Chapter 1: Introduction....4
Chapter 2: Getting Started....5
Routing mail traffic....5
Chapter 3: Deployment....5
Inbound Message Flow
....6
Outbound Message Flow....7
Chapter 4: The User Interface....8
Domain Selection Menu....8
The Overview Tab....9
System Status Display....9
Overview Reports....9
MessageIQ Settings Tab – System Level....10
Denied Incoming SMTP Hosts....11
Whitelist Configurations....12
Greylisting....14
Realtime Block Lists....15
Reverse-Path DNS Checks....16
Redlisting....17
Unknown Sender Delay....19
Anti-Spam Settings....20
Anti-Virus Settings....21
System Filters....24
Quarantine Options....25
MessageIQ Configurations Tab – Domain Level....28
....28
Whitelist Configurations....29
Unknown Sender Delay....31
Anti-Spam Settings....31
Anti-Virus Settings....33
Domain Filters....34
Address Filters....35
Quarantine Options....36
SMTP Settings Tab – System Level
....38
Allowed Outgoing Hosts....41
Mail Services....42
Message Footers....42
Miscellaneous Settings....43
SMTP Destinations....44
SMTP Settings – Domain Level....45
Accepted Addresses....46
Domain Aliases....47
Honey Pots....47

MS Exchange Connector 48
Message Footers 49
SMTP Routes 49
System Settings Tab 51
Alert E-mail Addresses 52
Branding 53
Date and Time Settings 54
External System Logging 55
Login Accounts 56
Login IP Restrictions 57
Maintenance 57
Network Configuration 58
Network Troubleshooting 59
Remote System Backups 59
SSL Settings 60
Shutdown / Restart 62
Support Admin Login 63
System Status 63
..... 63
System Updates 64
..... 64
Technical Contact List 65
The Reports Tab 65
Custom Emailed Reports 65
Report Scheduling 65
Emailed Report Addresses 67
Queue Status 68
Statistics 70
Chapter 5: Custom Filters 71
Filter Options 71
Chapter 6: Queue Management 75
Chapter 7: Frequently Asked Questions 77
Chapter 8: Service and Technical Support 80

Chapter 1: Introduction

MailFoundry™ is a full-featured email filtering appliance which includes the human intelligence powered MessageIQ email filtering engine. Using a technology called Spam Profiles; the MessageIQ engine is extremely accurate in its spam detection.

What are Spam Profiles?

Spam profiles are highly targeted profiles of a sender of spam, an individual spam message or a collection of spam messages. Spam Profiles are created by our human editors, in real-time, to provide the quickest response to new spam outbreaks. Spam Profiles are updated every five minutes and are automatically sent to your MailFoundry appliance.

Models Covered In This Manual

This user manual covers the following versions of the MailFoundry Appliance

MailFoundry 8100
MailFoundry 6100
MailFoundry 4100
MailFoundry 2100
MailFoundry 1150

Requirements

Before installing your MailFoundry appliance, you will need to verify that your configuration meets the following requirements.

You must have a pre-configured SMTP compatible mail server (Microsoft Exchange, Qmail, etc.)
You must have the ability to modify your DNS information (MX Records)
If you are using a firewall system, you must be able to configure your firewall to allow traffic to various TCP/IP ports.

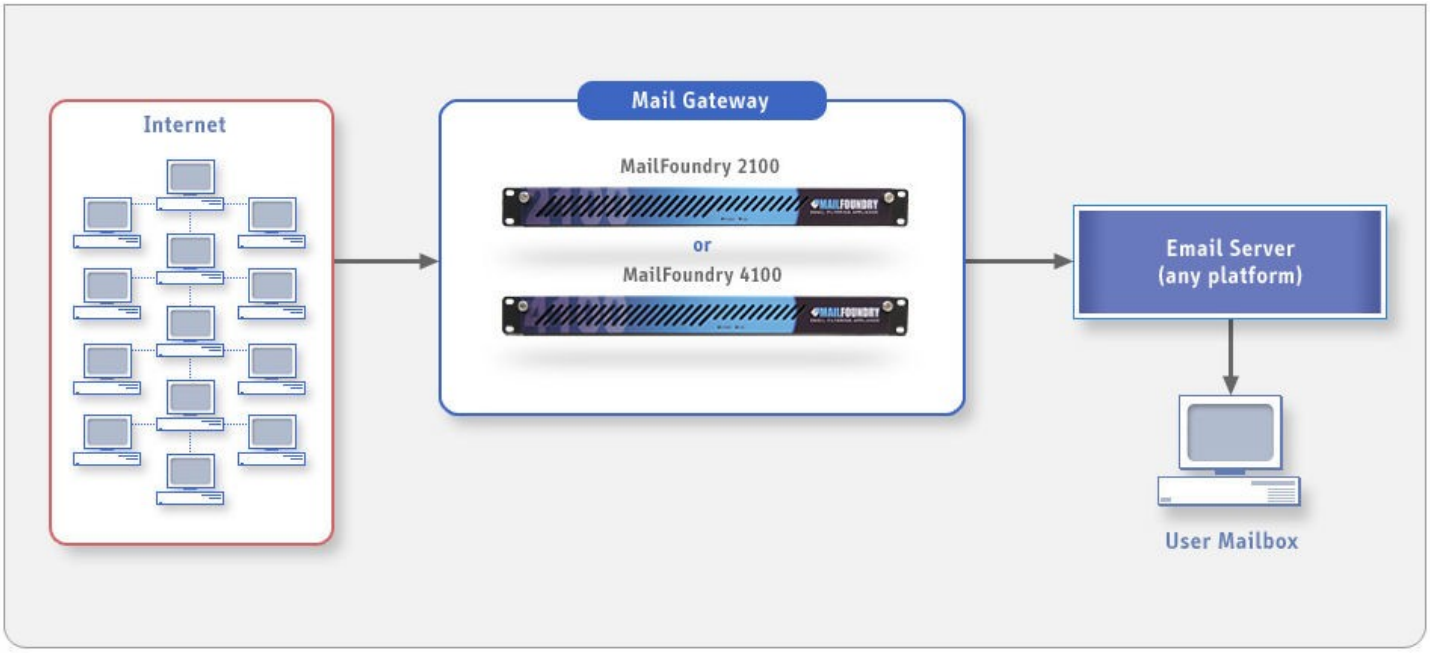
Chapter 2: Getting Started

Routing mail traffic

You will need to make changes to the DNS records for each domain that will be filtered by the MailFoundry Network Appliance.

You will need to add a new MX record that will point to the MailFoundry. You should also remove any current MX records that point to your target mail server, as this would allow spam and viruses to reach your server without protection.

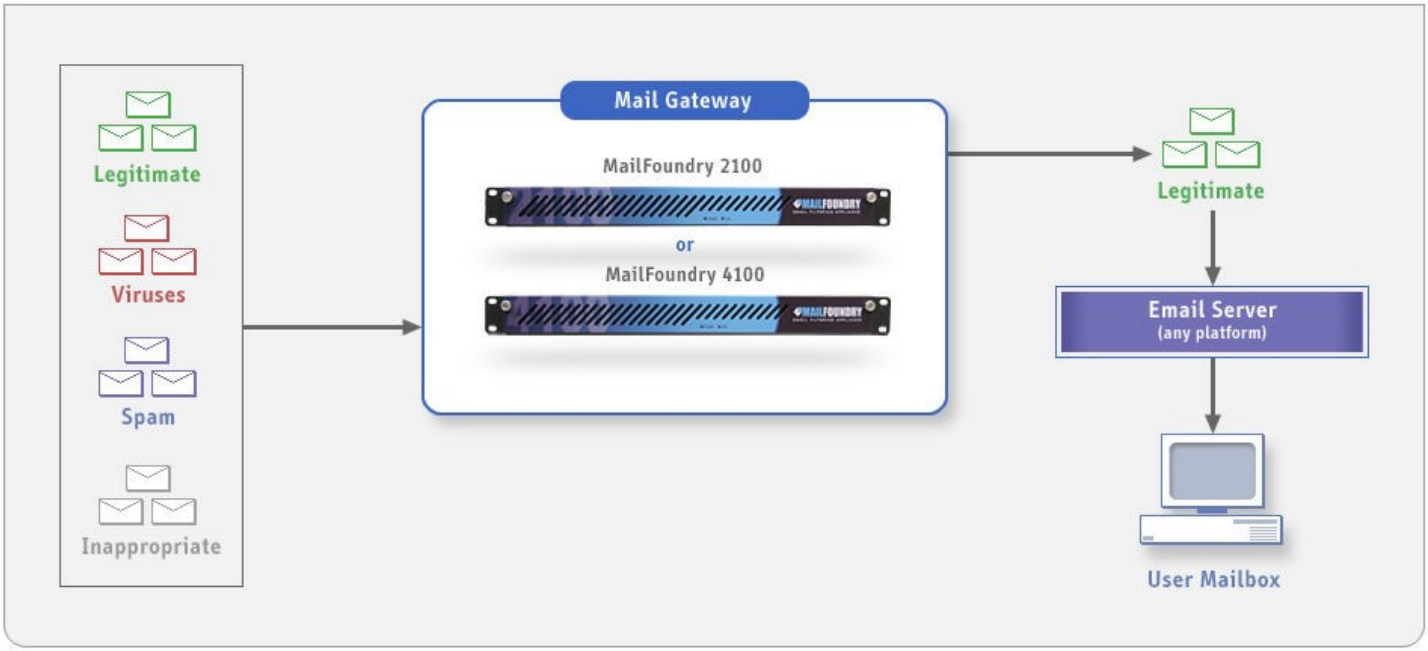
Chapter 3: Deployment



Your MailFoundry appliance is designed to act as mail "gateway" for all of your inbound and optionally, your outbound email traffic. MailFoundry secures your internal SMTP servers by processing all communications with external SMTP servers.

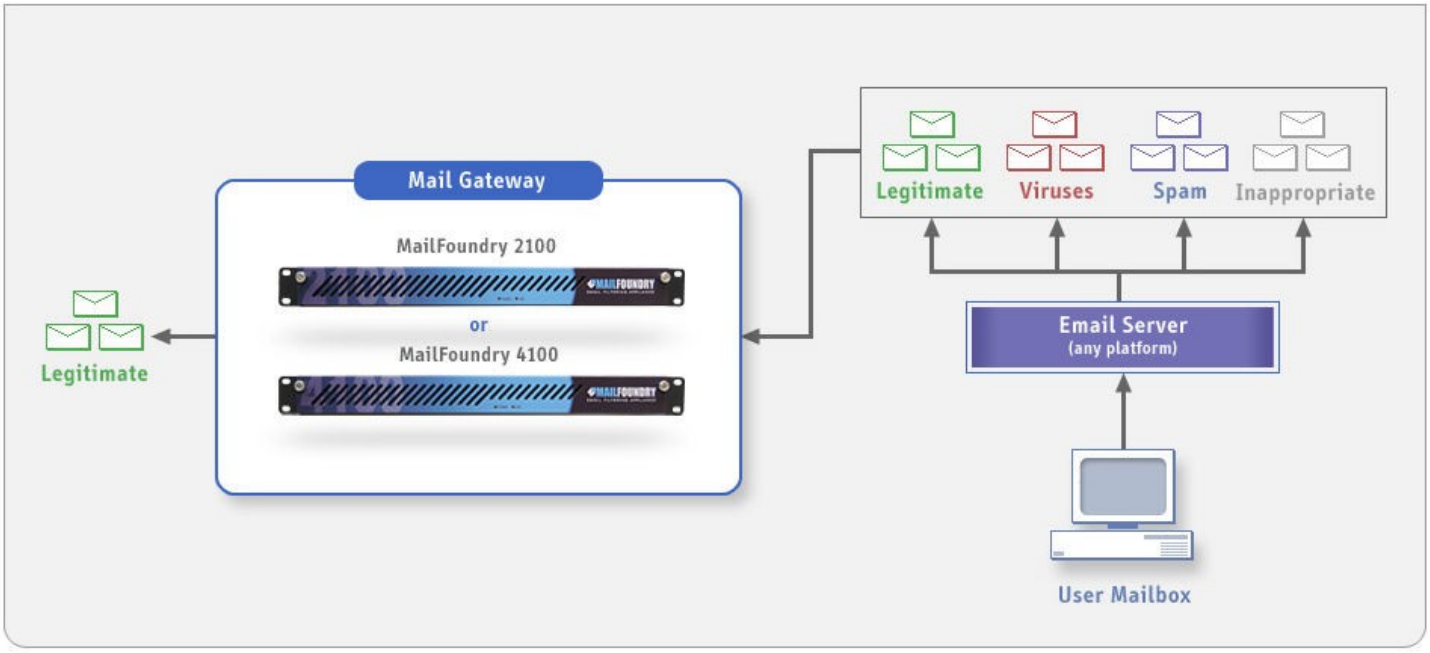
Because the SMTP server technology, hMail, included inside the MailFoundry appliance is a custom designed SMTP server, it is immune to common SMTP based worms designed to attack SMTP servers such as Microsoft Exchange or SendMail.

Inbound Message Flow



Each domain that will be filtered by the MailFoundry appliance will require modification to the domain's MX records. The only MX records that should be listed would be the hostname of your MailFoundry network appliance. You should not list any secondary MX records that are not protected by a MailFoundry appliance as the domain will then be unprotected and spam will pass to your back-end SMTP server.

Outbound Message Flow



Outbound message scanning provides your organization with extra protection from being party to the sending of viruses or spam as well as helps you to maintain standards of content sent from your network.

Internal Infection
Many companies have found that employees can easily bring infected computers or install infected applications which can send large amounts of spam or virus infected messages, in many cases, the company is not even aware of the issue until it is reported by a 3rd party.

Content Policy Management
Your MailFoundry appliance allows you to apply custom filters to outbound messages based on the content of the message. This solution is often effective in keeping non-appropriate or confidential information from being sent from your network. When used for outbound scanning, the MailFoundry appliance applies system level filters and whitelists to outbound messages.

Outbound Deployment
The first step in configuring your MailFoundry appliance for outbound scanning is to add the TCP/IP addresses of your SMTP server(s) to the Allowed Outgoing Hosts under the SMTP Settings tab.

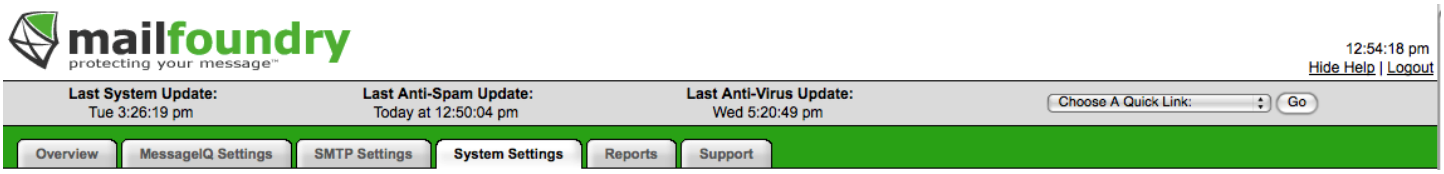
Next, configure your SMTP server to use a "Smart Relay" server. When asked for a TCP/IP addresses or host name, enter the TCP/IP address or host name of your MailFoundry appliance.

No changes are required for your users SMTP or POP3 message settings in their email client.

Chapter 4: The User Interface

To access the user interface of your MailFoundry appliance, you will need to use a supported web browser such as Internet Explorer, Netscape, Mozilla or Firefox. Point your web browser to:

http://<MailFoundry Hostname>.<Your Domain>.com
Example: http://mailfoundry.yourdomain.com



You have two options for navigation when in the MailFoundry user interface. You may use the collection of tabs located on the top portion of the screen to enter one of the following sections or you may choose the quick navigation drop down list located on the upper right of the screen.

User Interface Sections	
Overview	This tab is the default view when you enter the MailFoundry appliance's user interface. Included in this tab are several graphical reports illustrating your email traffic and filtering statistics.
MessageIQ Configurations	This tab allows you to configure the MessageIQ filtering engine. Options found in this tab include the configuration of anti-spam and anti-virus services as well as content filtering settings.
SMTP Settings	This tab allows you to configure SMTP related settings such as the domains you will accept email for, the hosts that can send mail outbound and the list of internal mail servers which will receive email traffic.
System Settings	This tab allows you to configure system related features including network configurations, external logging, and system updates.
Reports	This tab allows you to configure reporting features such as custom statistical reports. Under this tab, you can view your collected statistics and manage your message queues.
Support	This tab provides you with information on how to receive technical support for your MailFoundry appliance.

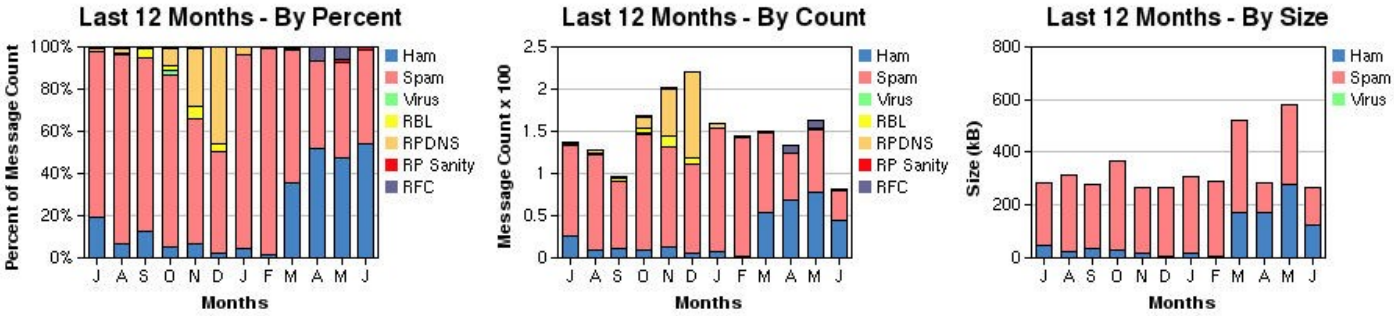
Domain Selection Menu

On many of the user interface screens, you will notice a domain selection drop-down menu. Using this menu will allow you to change from a system-wide global scope to a domain specific scope. Many options are only available when using the system level or domain level views.

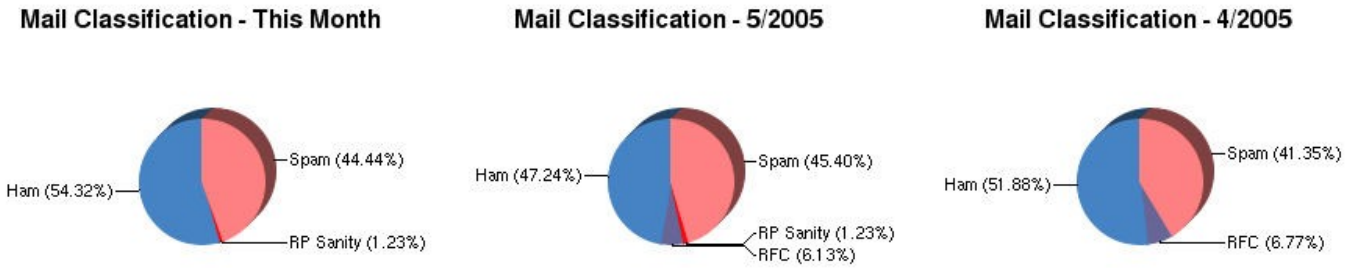
The drop down menu will change to a search box when the number of domains exceeds 20 domains.

The Overview Tab

System Status Display



Last 3 Months

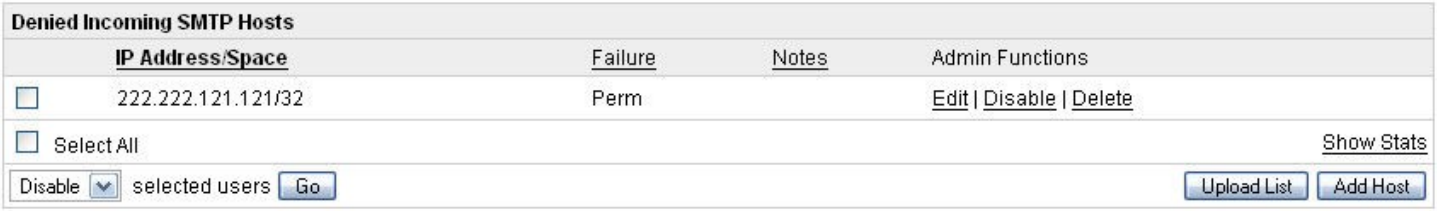


Overview Reports	
Last 12 Months By Percent	This graphic shows you the message volume by percentage divided by message type, such as Ham (valid messages), spam, and viruses.
Last 12 Months By Count	This graphic shows you the message volume by total count divided by message type, such as Ham (valid messages), spam, and viruses.
Last 12 Months By Size	This graphic shows you the message volume by total size of mail divided by message type, such as Ham (valid messages), spam, and viruses.
Mail Classification	These graphics shows you the message volume by percentage divided by message type, such as Ham (valid messages), spam, and viruses during the current month, last month and month before last.
Virus Classification	These graphics shows you the top three viruses detected by percentage of all infected messages during the current month, last month and month before last.

MessageIQ Settings Tab – System Level

Menu Structure	
Denied Incoming Hosts	This option allows you to block sending SMTP servers by IP address or IP block.
Whitelists	This option allows you to configure system-wide Whitelists.
Greylisting	This option causes temporary rejections of email to help defeat certain kinds of spam attacks.
Realtime Block Lists	This option allows you to configure third party Realtime Block List services to be used by your MailFoundry appliance.
Reverse-Path Checks	This option allows you to enable or disable Reverse-Path DNS Checks and Reverse-Path Sanity Checks.
Redlisting	Redlisting is an option that helps to detect and block attacks by systems attempting to send to a large amount invalid users.
Unknown Sender delay	Unknown sender delay adds a user configurable delay to any message coming from a user it has never seen mail from before.
Anti-Spam Settings	This option allows you to configure, enable or disable the anti-spam portion of the MessageIQ engine.
Anti-Virus Settings	This option allows you to configure, enable or disable the anti-virus portion of the MessageIQ engine.
Unknown Sender Delay	Unknown sender delay is an option that allows emails from unknown addresses to be delayed for a period of time to allow for better spam detection.
System Filters	This option allows you to create, edit, enable or disable custom filters that affect the entire system.
Quarantine Options	This option allows you to configure, enable or disable the quarantine system. You may also set quarantine overrides and redirects.

Denied Incoming SMTP Hosts



Us
ac

A
To
below.

Field	Description
IP Address or Space	Enter the IP address or IP space in the following format: 123.123.123.123
IP Address Type	Select the type of listing you will be adding using the above IP address Options include a single IP address, IP block with bit mask or IP block with subnet mask. If you select to list an IP block with bit mask, enter the integer mask. If you select to list an IP block by subnet mask enter the subnet mask in the following format: 255.255.255.0
Failure Type	
Enabled	When this field is checked, the listed IP address or IP address block will be blocked. If unchecked, the sender may send mail to the appliance.
Notes	You can enter an internal description that will help you identify this entry or provide details as to why it was added.

Uploading a List of IP Addresses
To upload a text file containing a list of IP address, click on the "Upload List" button. When uploading a list, the list must contain a listing of one IP address or address group per line in one of the following formats:

Single IP (eg. 123.123.123.123)
IP block with integer mask (eg. 123.123.123.123/24)
IP block with subnet mask (eg. 123.123.123.123/255.255.255.0)

Searching for an IP Address
To search for a listed IP address, enter the IP address into the "Search for an IP" text field in the "Search" section and click on "Search".

Editing an IP Address
To edit an IP address, click on the "edit" link in the corresponding row within the main listing.

Enable, Disable or Delete an IP Address
To enable, disable or delete an IP address or group of IP addresses, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

View Usage Statistics

To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Whitelist Configurations

Your MailFoundry appliance includes a complete whitelisting system that gives you maximum flexibility. You may choose what sender may bypass a filtering technology and which filtering technology they may bypass. Whitelist entries created in this section are system-wide in scope.

Legend	Description
G	This entry will bypass Greylisting.
B	This entry will bypass the realtime block list check.
D	This entry will bypass the reverse path DNS check.
RD	This entry will bypass Redlisting.
M	This entry will bypass the maximum message size limit check.
R	This entry will bypass the strict RFC compliance check.
J	This entry will bypass the anti-spam filtering system.
V	This entry will bypass the anti-virus filtering system.
CS	This entry will bypass all custom system filters.
CD	This entry will bypass all custom domain filters.
CU	This entry will bypass all custom address filters.

Adding a New Entry
To add a new entry to the whitelist system, click on the "Add Entry" button. Fill in the fields as listed below

Field	Description
For messages matching this criteria - Originating IP	Enter the IP address or IP address block in the following format: 192.168.0.1 Address Type – Select the address type of either a single IP address, an address blocked with a bit mask (Example: /24) or an address block with a subnet mask (Example: 255.255.255.0).
For messages matching this criteria - "Mail From" Domain	Enter the full domain name of the sender (Example: Solinus.com).
For messages matching this criteria - "Mail From" Address:	Enter the full email address of the sender (Example: support@solinus.com).
Disable these filters	Select the filtering technologies you would like to disable. You can also choose "All but virus filtering disabled" to disable all checks but keep virus scanning active.
Comment	You can enter an internal description that will help you identify this entry or provide details as to why it was added.
Enabled	When this field is checked, the entry will be whitelisted. If unchecked, the entry will be filtered normally.

Uploading a List of entries
To upload a text file containing a list of entries, click on the "Upload Whitelist" button. When uploading a list, the list must contain a listing of one entry per line. You will want to create separate lists for addresses, IP addresses, and domains. Complete the selections for the file you are uploading. All entries in the file will be uploaded with these settings.

Editing an Entry
To edit an entry, click on the "Edit" link on the right in the corresponding row within the main listing.

Enable, Disable or Delete an Entry
To enable, disable or delete an entry or group of entries, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

To enable, disable or delete an individual whitelist, click the "Enable", "Disable", or "Delete links on the right in the corresponding row within the main listing.

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Greylisting

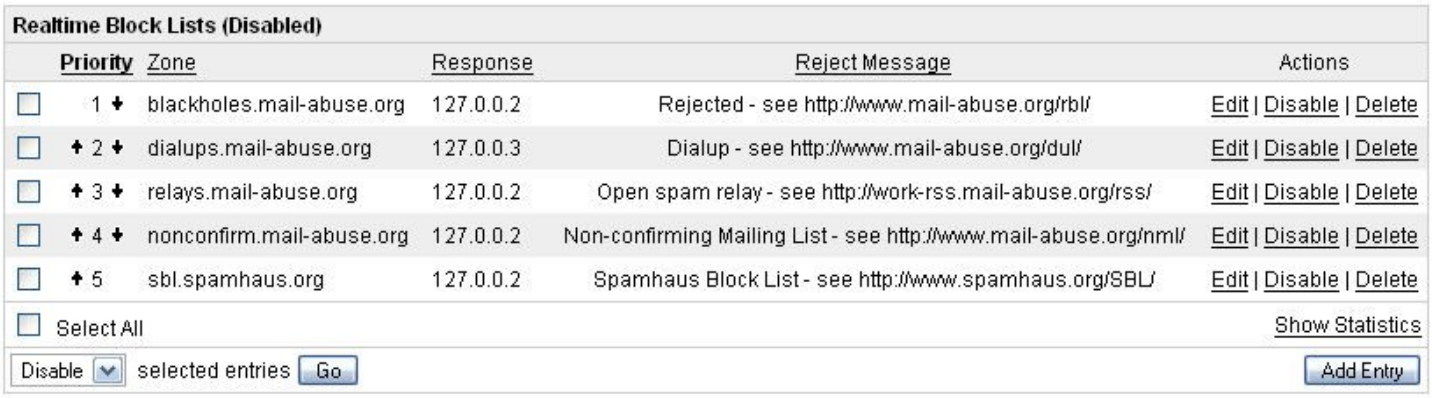
Greylisting is an additional level of blocking spam outside of MessageIQ. This feature works by looking at the IP a message has come from and the envelope sender and recipient. Once the connection is started it will receive a temporary failure for a period of time. After that time period, which is adjustable from the interface, messages from that IP with that exact sender and recipient will be allowed to deliver.

This works because all legitimate email servers are designed to reprocess mail in the event of a temporary failure. Spam hosts, however, do not usually attempt any retries.

The draw back to Greylisting is that not all mail servers will retry after an initial temporary failure quickly. Some servers could potentially wait hours before trying to resend the message and this can cause some delayed emails.

It is not advised to use Redlisting and Greylisting at the same time.

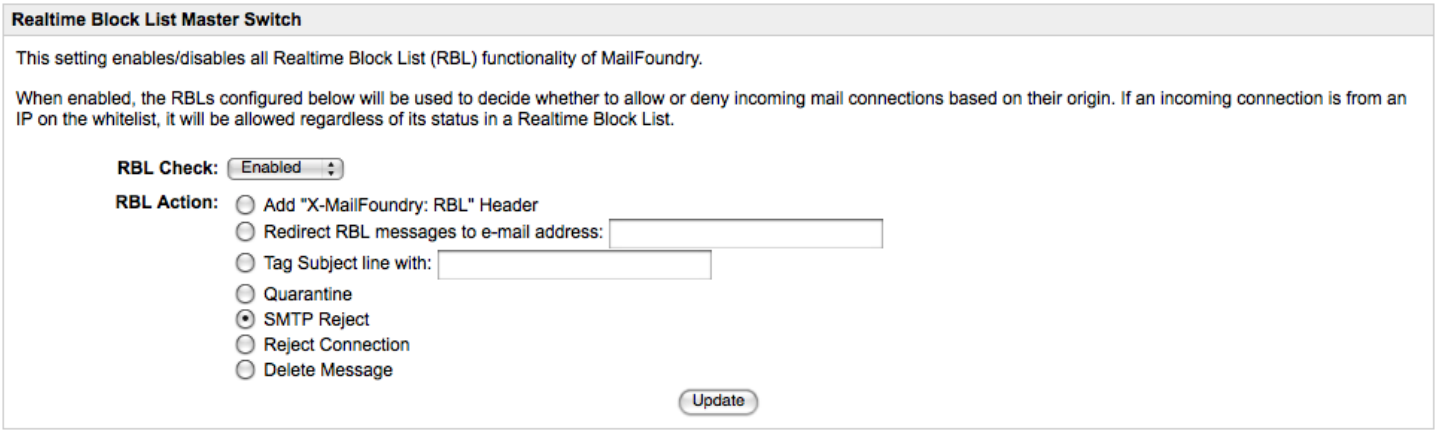
Realtime Block Lists


Realtime Block Lists (Disabled)
Priority
Zone
Response
Reject Message
Actions
1 blackholes.mail-abuse.org 127.0.0.2 Rejected - see http://www.mail-abuse.org/rbl/ Edit | Disable | Delete
2 dialups.mail-abuse.org 127.0.0.3 Dialup - see http://www.mail-abuse.org/dul/ Edit | Disable | Delete
3 relays.mail-abuse.org 127.0.0.2 Open spam relay - see http://work-rss.mail-abuse.org/rss/ Edit | Disable | Delete
4 nonconfirm.mail-abuse.org 127.0.0.2 Non-confirming Mailing List - see http://www.mail-abuse.org/nml/ Edit | Disable | Delete
5 sbl.spamhaus.org 127.0.0.2 Spamhaus Block List - see http://www.spamhaus.org/SBL/ Edit | Disable | Delete
Select All
Show Statistics
Disable
selected entries
Go
Add Entry

Realtime Block Lists, or RBLs, are realtime databases of known spam sources maintained by third parties. Your MailFoundry appliance can query configured RBLs and reject inbound mail if the source is listed within the RBL database.

****IMPORTANT NOTICE***
Solinus does not operate or manage RBL services and therefore cannot verify the integrity of the listings. Many third party RBL databases include large listings of major internet service providers, which can cause legitimate emails not to be delivered to your users.

Enable Realtime Block Lists


Realtime Block List Master Switch
This setting enables/disables all Realtime Block List (RBL) functionality of MailFoundry.
When enabled, the RBLs configured below will be used to decide whether to allow or deny incoming mail connections based on their origin. If an incoming connection is from an IP on the whitelist, it will be allowed regardless of its status in a Realtime Block List.
RBL Check:
Enabled
RBL Action:
Add "X-MailFoundry: RBL" Header
Redirect RBL messages to e-mail address:
Tag Subject line with:
Quarantine
SMTP Reject
Reject Connection
Delete Message
Update

RBLs are an optional technology that may be enabled and disabled as needed. To enable RBL processing select "Enable" from the "Master Switch" menu located on the listing page. Once RBL processing is enabled, you may enable or disable individual RBLs as needed.

Choose the action you would like to have the MailFoundry do if a message is coming from a source that is on a Real Time Block List. Click Update to save the settings.

Adding a New Entry
To add a new entry to the RBL system, click on the "Add Entry" button. Fill in the fields as listed below.

Field	Description
Zone	Enter the hostname of the RBL server to query (Example: zen.spamhaus.org)
Server Response	Enter the response codes for the RBL. You can get those from the website of the RBL (Example: www.spamhaus.org/zen). You can also use the 'any' wildcard response.
Reject Info. Message:	Enter a message that will be sent to the sending SMTP server notifying it of the failure.
Priority	Enter the Priority of this RBL list in relation to other lists you have configured. The priority is the order in which the RBLs are checked.

Editing an Entry
To edit an entry, click on the "Edit" link in the corresponding row within the main listing.

Enable, Disable or Delete an Entry
To enable, disable or delete an entry or group of entries, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either Enable, Disable or Delete from the drop down list located at the lower left of the list. Finally, click on "Go".

To enable, disable or delete an individual entry, click "Enable", "Disable", or "Delete to the right on the corresponding line of the entry.

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Reverse-Path DNS Checks

Reverse-Path Checks
The following options will perform various checks on the domain in the sender's address, as listed in the SMTP Envelope From.
Reverse-Path DNS Check
Disabled
Reverse-Path Sanity Check
Enabled
Update

MailFoundry includes a unique DNS based verification system called "Reverse-Path DNS". Using this system, your MailFoundry appliance will check all incoming messages to make sure that the sender's domain is valid.

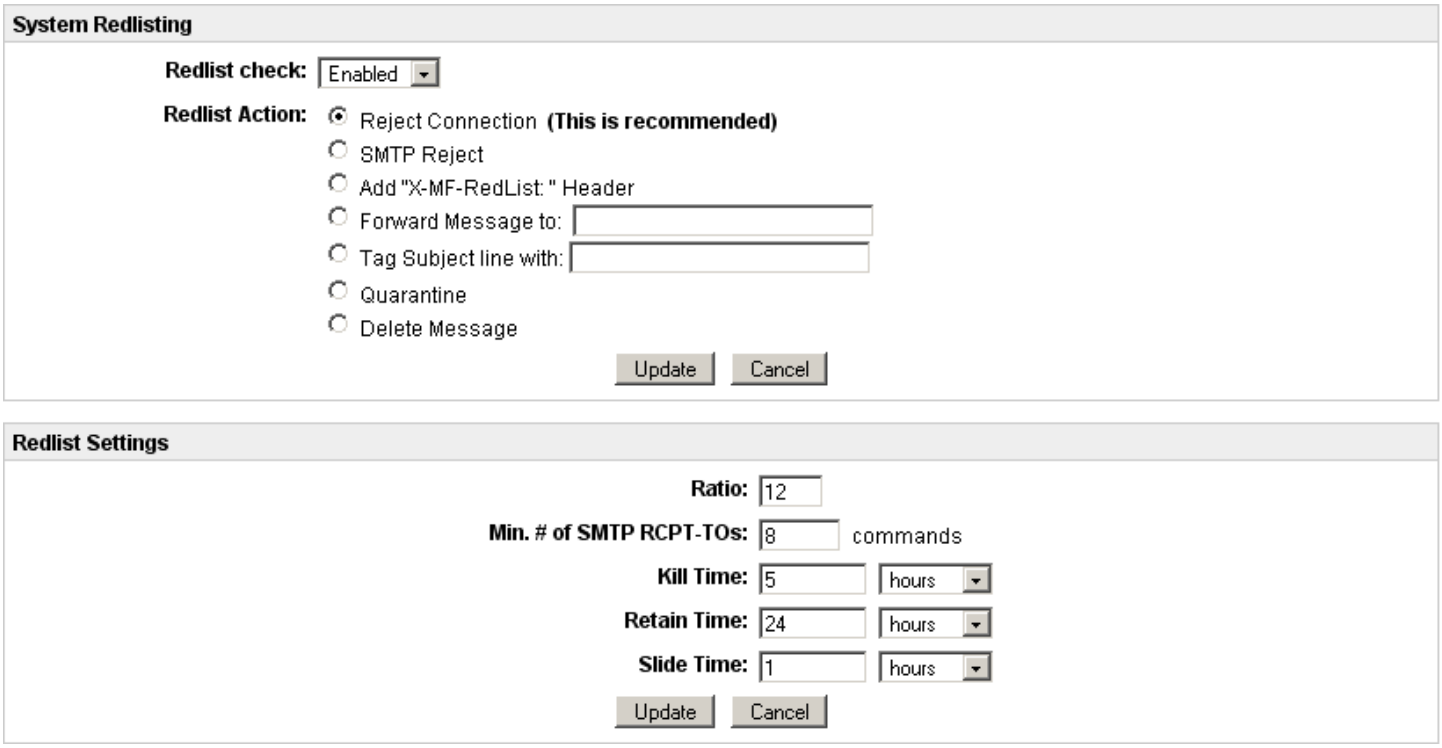
First, the MailFoundry appliance will check to see if there is a valid Mail Exchange or "MX" record for the sender's domain. If the MailFoundry appliance is unable to find a valid record, it will next search for a valid "A" record for the domain.

If both lookups fail, the message will be rejected.

An additional check can be preformed called, "Reverse-Path Sanity Check". This check will verify that there is a valid "MX" record for the sender's domain and that it does not resolve to localhost (127.0.0.1), which could cause stability issues such as mail loops.

Both of these options can be enabled or disabled as needed.

Redlisting



Redlisting relies on the assumption that spammers make a number of attempts to deliver email to email addresses that do not exist.

Using this assumption, we constructed a methodology for measuring the rate at which attempts are made to send emails to unknown addresses. Using that data we can compare the rate of good attempts to bad attempts over a period of time to a user defined ratio. If the ratio of bad attempts to good attempts seen from a particular IP address exceeds the user defined ratio, that IP enters a state that is said to be "Redlisted". An IP stays Redlisted for a user defined period of time and any connections or emails from that IP address is subjected to the user configurable action.

To enable Redlisting, select “Enabled” from the Redlist Check drop down menu.

Select the desired action to be taken when a message is RedListed.

Action	Description
Reject Connection	This option will send a permanent rejection to the RedListed IP when it tries to connect.
SMTP Reject	This option will send a permanent rejection to the RedListed IP after it sends the To: and From: addresses.
Add "X-MF-RedList: " Header	This option will add an X-MF-RedList: entry to the header of the message coming from RedListed IP’s.
Forward Message to:	This option will forward messages coming from RedListed IP’s to a specific email address.
Tag Subject line with:	This option will add the desired text to the Subject line of the messages coming from a RedListed IP.
Quarantine	This option will add messages from RedListed IP’s to the Quarantine Queue.
Delete Message	This option will delete messages coming from RedListed IP’s.

Redlist Settings

The default settings are usually the best options for most installations and it is recommended to start by using the defaults.

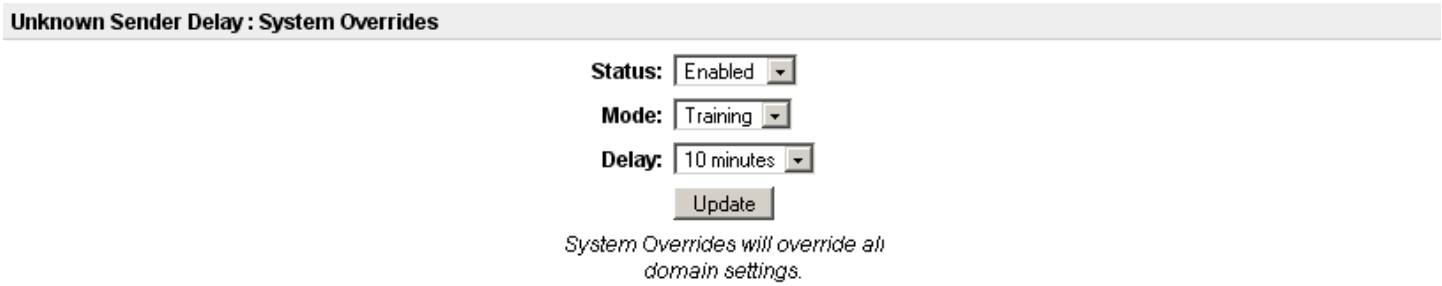
Setting	Description
Ratio	When a connecting IP sends more bad rcpt to addresses than good, the system will start building a ratio. This ratio is built using the following formula: (good addresses/bad addresses) * 100
Min. # of SMTP RCPT-TOs	This is the number of addresses it watches to get the sampling to create the ratio.
Kill Time	This is the amount of time the IP will be RedListed.
Retain Time	This is how long to watch for the incoming messages for the IP.
Slide Time	This is how long to keep the data if the minimum number of RCPT-TOs is not met.

The quickest way to check the current status of a host is to use the "Redlist Search" which is available in the Redlisting tab under the MessageIQ settings. Enter the IP address of the host you wish to check into the text box and click the "Search Redlisted IP's" button.

If the appliance has received a connection from the host recently and Redlisting is enabled, the current statistics for that IP are displayed.

Field	Description
Good	This field represents the number of RCPTTOs That were received from an IP and were valid within the last period of stastic collection.
Bad	This field represents the number of invalid RCPTTOs within that time period
RedList count	This field indicates the number of times in the current month the IP address has been connected to the appliance while redlisted.
Percent Redlisted	This field is calculated from the RedList Count and the Connection Count.
Status	Will indicate the current status of the host as calculated using the user defined settings. Possible Values in this column are "not RedListed" and "RedListed".

Unknown Sender Delay



Unknown Sender Delay is a method of handling email from new senders that can greatly help cut down spam. This process works by putting any email from an address that has never sent mail to that MailFoundry appliance before to be delayed by a configurable period of time. This allows the appliance more time to get updated spam rules that may match the incoming spam message.

To use this feature we recommend enabling it in training mode for 3 to 5 days. In that time it starts building a list of addresses that normally send email to the appliance. After that time period it can be changed to delay mode.

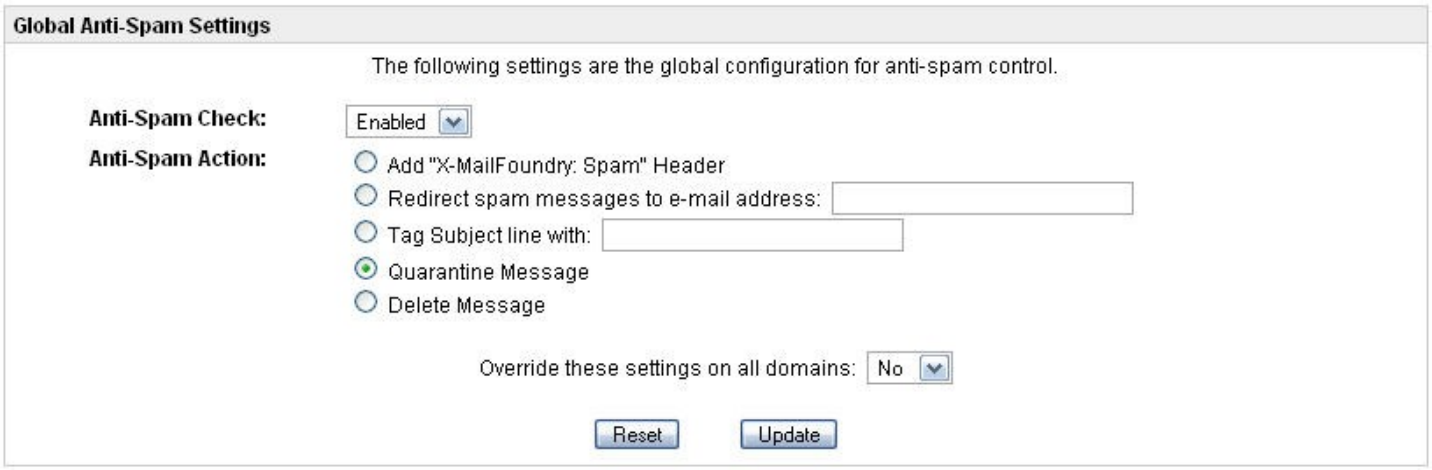
After a sender has been added to the Unknown Sender Delay database, future emails received from that sender are not subject to delay.

If you make changes and click Update on the system level, you will be prompted with:

Are you sure you want to overwrite all domains with the following settings?

Clicking the Update button will set all domains with the new settings. This is a one time only override of the domain settings. You can then go to the specific domains and make changes that will affect only the domain selected. *New domains will not automatically be set to Delay mode*.

Anti-Spam Settings



Field	Description
Anti-Spam Check	This option will allow you to enable or disable anti-spam filtering for your entire system.
Anti-Spam Action	There are several options for defining how detected spam messages are handled. Add "X-MailFoundry: Spam" Header – This option will place a header within the message that can be used for filtering with an email client such as Microsoft Outlook. Redirect spam messages to e-mail address – This option will send all detected spam messages to an email address you define. Tag Subject line with – This option will add a tag at the beginning of the subject line of all detected spam (Example: [SPAM]). Quarantine Message – This option will place the message into Quarantine system. Delete Message – This option will delete all detected spam without notification.
Override these settings on all domains:	When this option is set to "No", all domain level settings remain when you modify system level settings. When this option is set to "Yes", all domain level settings are replaced with the new system level settings.

Per-User Overrides

Note: the '*' used here is strictly a placeholder. It is not intended to indicate that a wildcard can be used.

Using the per-user override system, you can configure specific users, by email address, to have different anti-spam setting then the defaults. To add a new override, click on the "Add Override" button in the lower right of the main view.

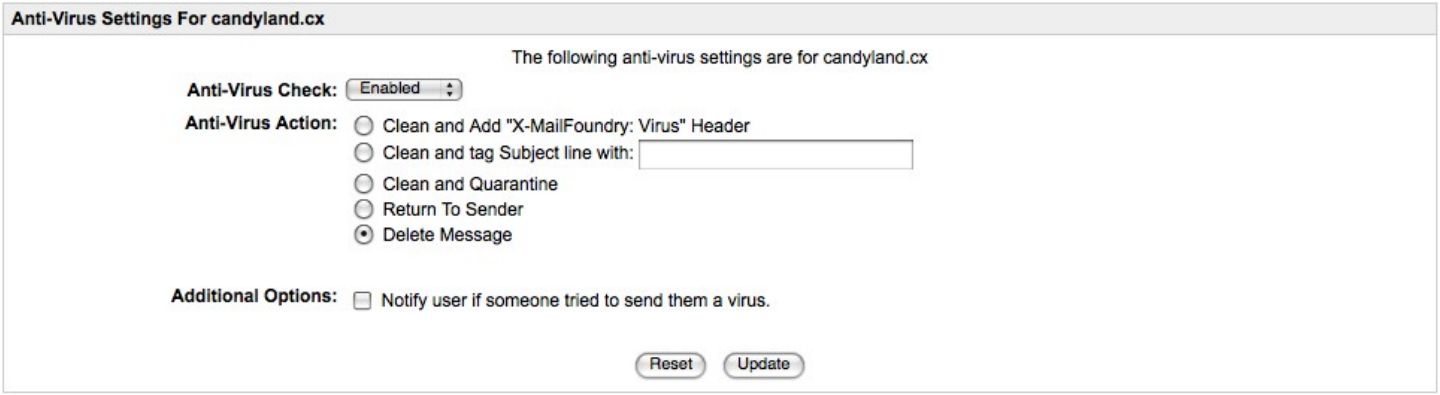
You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

*Note: wildards can not be used.

Editing a Per-User Override
To edit a per-user override, click on the "edit" link in the corresponding row within the main listing.

Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides".

Anti-Virus Settings



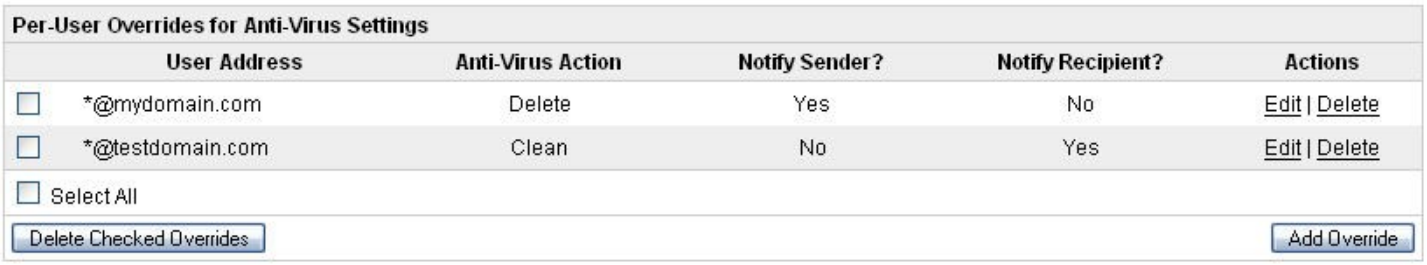
This screen allows you to configure your anti-virus options. Settings configured on this screen are system-wide unless a domain has been given domain specific settings.

Configuring Options

To modify your anti-virus settings, edit the following fields and click on "Update". It is important to remember that settings will not override domain specific settings unless you select "Override these settings on all domains" before saving.

Field	Description
Anti-Virus Check	This option will allow you to enable or disable anti-virus filtering for your entire system.
Anti-Virus Action	There are several options for defining how detected virus infected messages are handled. Clean and add "X-MailFoundry: Virus" header – This option will clean the infected message and place a header within the message will can be used for filtering with an email client such as Microsoft Outlook. Clean and tag subject line with – This option will clean the infected message and add a tag at the beginning of the subject line of the cleaned message (Example: [VIRUS]). Clean and Quarantine Message – This option will clean the infected message and place the message into Quarantine system. Return To Sender – This option will return the infected message back to the sender. Delete Message – This option will delete all infected messages without notification.
Notify User	This option will send a notification message to the recipient of the infected message.
Override these settings on all domains:	When this option is set to "No", all domain level settings remain when you modify system level settings. When this option is set to "Yes", all domain level settings are replaced with the new system level settings.

Per-User Overrides



Note: the '*' used here is strictly a placeholder. It is not intended to indicate that a wildcard can be used.

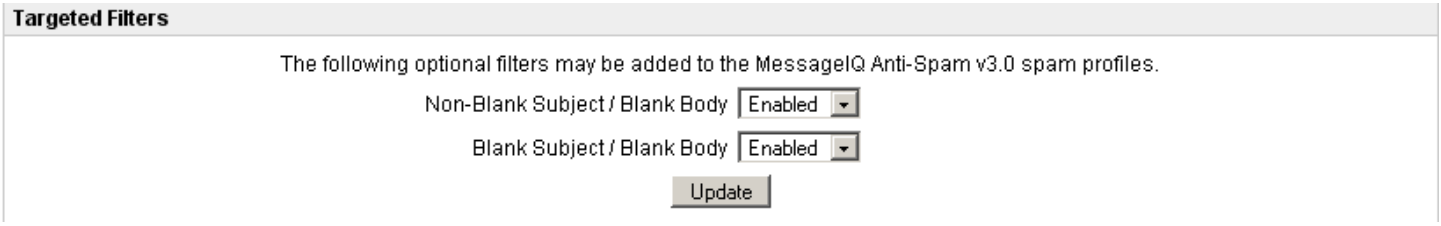
Using the per-user override system, you can configure specific users, by email address, to have different anti-virus setting then the defaults. To add a new override, click on the "Add Override" button in the lower right of the main view. Please note, wildcard characters can not be used.

You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

Editing a Per-User Override
To edit a per-user override, click on the "edit" link in the corresponding row within the main listing.

Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides".

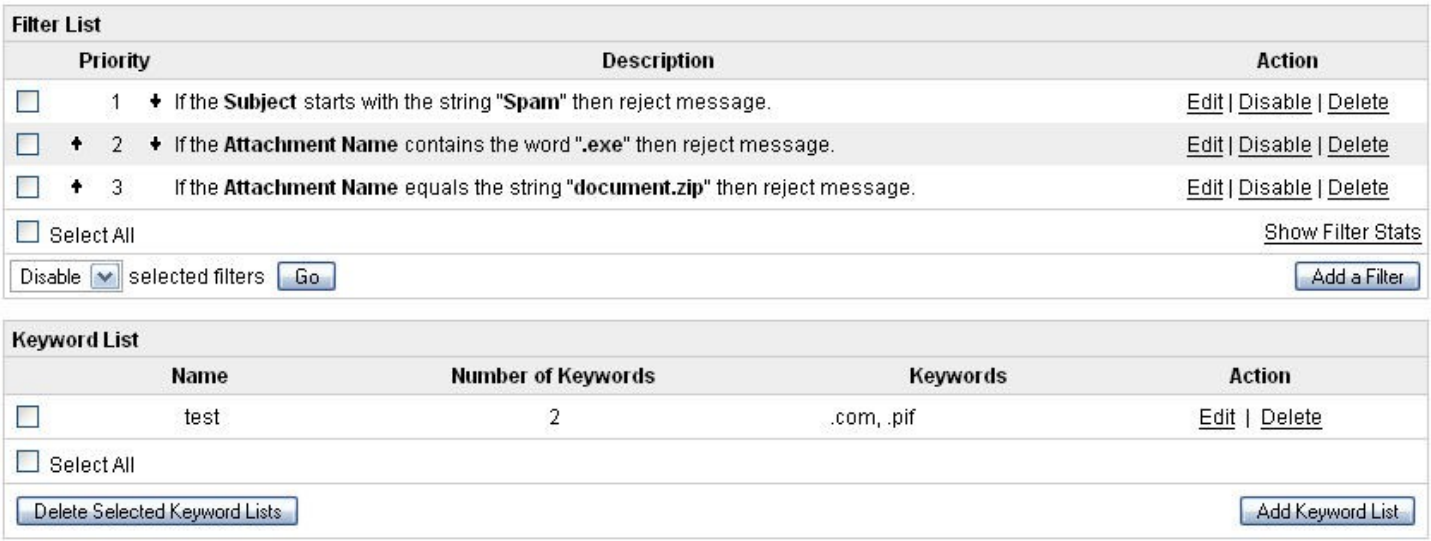
Targeted Filters


Targeted Filters
The following optional filters may be added to the MessageIQ Anti-Spam v3.0 spam profiles.
Non-Blank Subject / Blank Body
Enabled
Blank Subject / Blank Body
Enabled
Update

Targeted Filters are special filters that fall into a grey area of filtering outside the scope of normal spam profiles and may not be well suited for your needs. These rules have been added as an optional feature in MessageIQ Anti-Spam v3.0 as they could cause an unacceptable false positive rate for some customers.

Targeted Filters are designed to combat a type of spam attack that involves having all the information in the subject and nothing in the body or the entire message including subject being blank. Targeted Filters are very effective for defeating this type of email but it can cause false positives for senders who only put something in the subject and leave the body of the email blank as some do with test emails.

System Filters



MailFoundry includes a full-featured custom filters system. Using custom filters, you can create filters based on content of inbound and outbound messages. Filters may have a system level scope, domain level scope or user level scope.

Creating a Custom Filter
For details on the context of custom filters, see Chapter 5 – Custom Filters. To create a new custom filter, click on "Add a Filter". Next, enter all required fields and finally, click on "Create Filter".

Editing a Custom Filter
To edit a custom filter, click on the "edit" link in the corresponding row within the main listing.

Enable, Disable or Delete a Filter
To enable, disable or delete a filter or group of filters, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Changing a Custom Filters Priority
To change the priority of a custom filter, click on either the "Up" arrow or "Down" arrow in for the custom filter on the main view screen.

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Keyword Lists
Your MailFoundry appliance has the ability to filter messages based on a list of keywords you enter or upload. Keyword filtering is effective in blocking message based on the content however using this system can create false-positive detections.

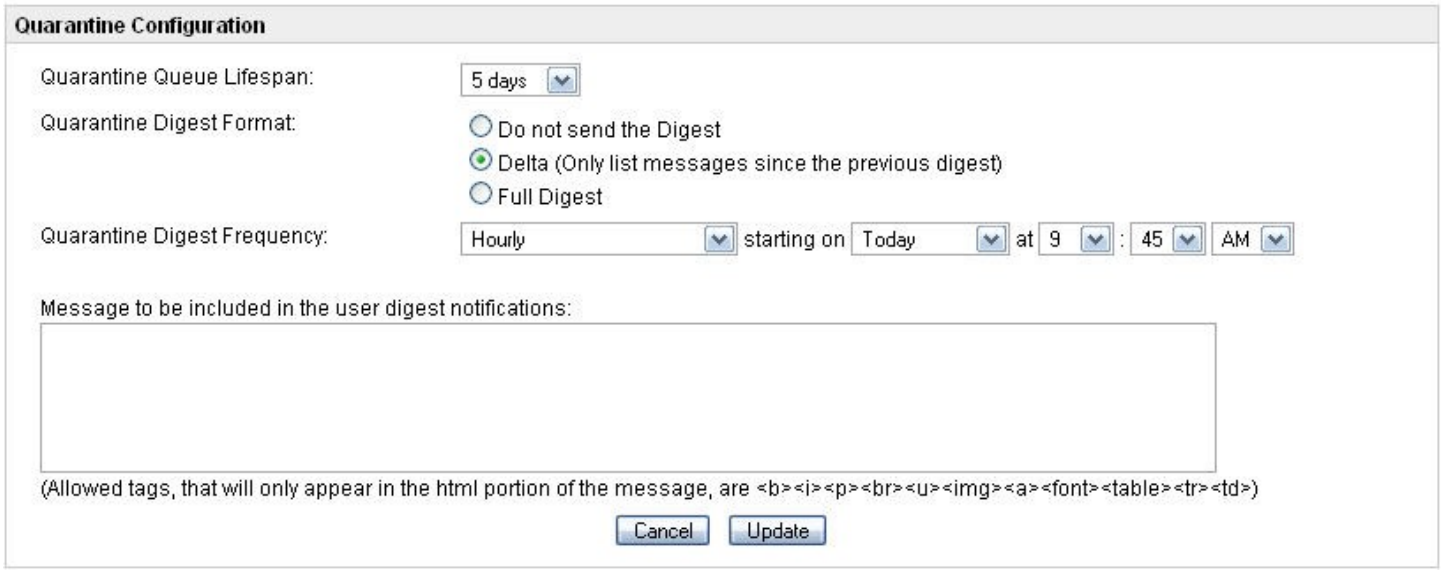
Once you have created your keyword list, you will need to create a custom filter that will utilize the keyword list.

Manually Entering a Keyword List
To manually enter a keyword list, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: badwords"). Now, enter the keywords in the keyword list field, one per line. When completed, click on "Create".

Uploading a Keyword List
To upload a previously created list of keywords, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: badwords"). Now, click on the "Browse" button. A directory listing will be displayed that will allow you to locate the saved file on your computers disk drive. Make sure the saved file lists the keywords, one per line. Once you have selected the file, click on "Create". Your file will be uploaded and your keyword list will be created.

Deleting a Keyword List
To delete a keyword list or group of keyword lists, click on the checkbox next to the entries you would like to remove. Next, click on "Delete selected keyword lists".

Quarantine Options



Your MailFoundry appliance includes a full-featured quarantine system. Although it is rare to have a false-positive message, using the quarantine system will give your email users the ability to view detected spam messages. You may also choose to have cleaned, virus-infected messages included in the quarantine system. Another unique feature your MailFoundry appliance offers is the ability to quarantine messages based on custom filters.

Configuring Options
To modify your quarantine settings, edit the following fields and click on "Update".

Field	Description
Quarantine Queue Lifespan	This option will allow you to set the number of days messages will remain active in the quarantine system between one and 45 days.
Quarantine Digest Format	This option will allow you to set the format of the quarantine digest messages mailed to your email users. Do not send the Digest would stop the digests from being sent. Delta will include only messages put in the Quarantine Queue since the last digest was sent. Full Digest will include all messages currently in the Quarantine Queue.
Quarantine Digest Frequency	This option will allow you to define the frequency of which digest messages are sent to users. You may choose to send the digests once per hour, once per day including weekends, or once per day excluding weekends.
Message to be included in the user digest notifications	This option will allow you to define a custom message which will be included with the digest messages. You may include the following HTML tags for formatting: <b> <i> <p> <u> <img> <a> <font> <table> <tr> <td>

Per-User Overrides

Using the per-user override system, you can configure specific users, by email address, to have different quarantine setting then the defaults.

To add a new override, click on the "Add Override" button in the lower right of the "Overrides for Quarantine Settings" box.

You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

Editing a Per-User Override
To edit a per-user override, click on the "Edit" link in the corresponding row within the main listing.

Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides" in the lower left of the "Overrides for Quarantine Settings" box.

Digest Redirections

A digest redirection allows you to redirect the digest messages for a specific email address to another email address. This is often beneficial when you have an alias which multiple users answer and you only need one person who is a member of the alias to manage the quarantine digests.

To add a new redirection, click on the "Add a Digest Redirection" button in the lower right of the "Digest" box.

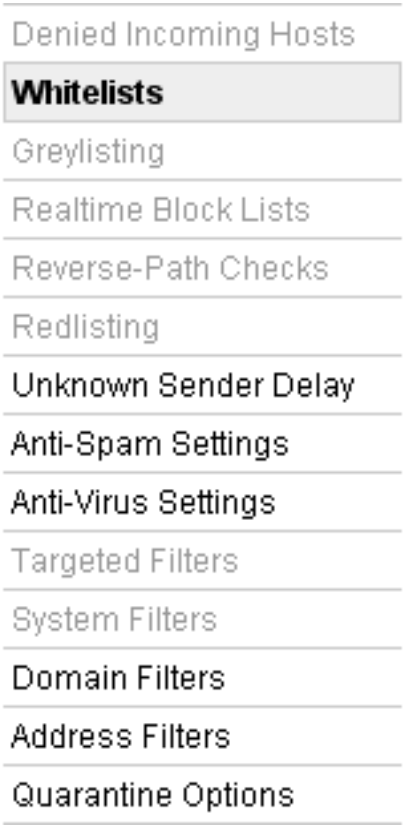
Enter the email address that you would like to redirect digest messages for. Next, enter the destination email address who will manage the quarantine for the redirected address. Finally, click on "Add Digest Redirection" to save you entry.

Editing a Digest Redirection
To edit a digest redirection, click on the "edit" link in the corresponding row within the main listing.

Deleting Digest Redirections
To delete digest redirections, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Selected Digest Redirections" in the lower left of the "Digest Redirections" box.

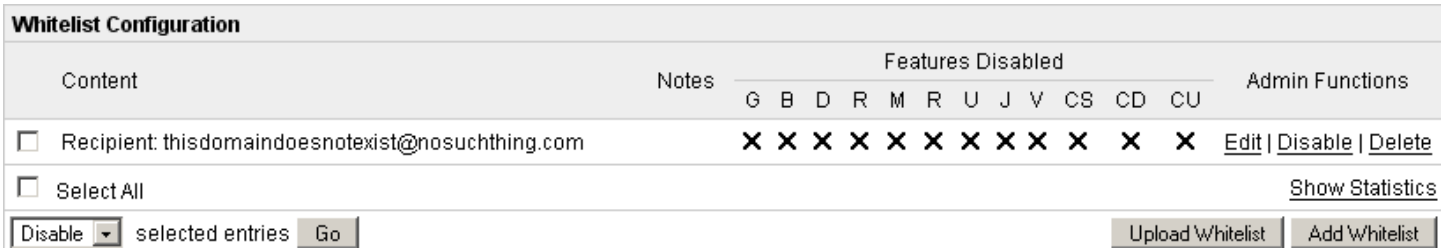
MessageIQ Configurations Tab – Domain Level

The MessageIQ tab allows you to set options related to the MessageIQ filtering engine. When you select a domain from the domain selection menu, your settings only affect that domain. You will notice that system level options are not displayed and several domain level only options are now displayed.



Menu Structure	
Whitelists	This option allows you to configure domain level Whitelists.
Unknown Sender Delay	This option allows you to configure Unknown Sender Delay
Anti-Spam Settings	This option allows you to configure, enable or disable the anti-spam portion of the MessageIQ engine.
Anti-Virus Settings	This option allows you to configure, enable or disable the anti-virus portion of the MessageIQ engine.
Domain Filters	This option allows you to create, edit, enable or disable custom filters that affect only the selected domain.
Address Filters	This option allows you to create, edit, enable or disable custom filters that affect a single user address in the selected domain.
Quarantine Options	This option allows you to configure, enable or disable the quarantine system for the selected domain. You may also set quarantine overrides and redirects.

Whitelist Configurations



Your MailFoundry appliance includes a complete whitelisting system that gives you maximum flexibility. You may choose what sender may bypass a filtering technology and which filtering technology they may bypass. Whitelist entries created in this section are domain specific in scope.

Legend	Description
G	This entry will bypass the Greylisting check
B	This entry will bypass the realtime block list check
D	This entry will bypass the reverse path DNS check
RD	This entry will bypass the Redlisting check
M	This entry will bypass the maximum message size limit check
R	This entry will bypass the strict RFC compliance check
U	This entry will bypass the Unknown sender delay check
J	This entry will bypass the anti-spam filtering system
V	This entry will bypass the anti-virus filtering system
CS	This entry will bypass all custom system filters
CD	This entry will bypass all custom domain filters
CU	This entry will bypass all custom address filters

Adding a New Entry
To add a new entry to the whitelist system, click on the "Add Entry" button. Fill in the fields as listed below

Field	Description
For messages matching this criteria - Originating IP	Enter the IP Address or IP address block in the following format: 192.168.0.1 Address Type – Select the address type of either a single IP address, an address blocked with a bit mask (Example: /24) or an address block with a subnet mask (Example: 255.255.255.0).
For messages matching this criteria - "Mail From" Domain	Enter the full domain name of the sender (Example: Solinus.com).
For messages matching this criteria - "Mail From" Address:	Enter the full email address of the sender (Example: support@solinus.com)
Disable these filters	Select the filtering technologies you would like to disable. You can also choose "All but virus filtering disabled" to disable all checks but keep virus scanning active.
Comment	You can enter an internal description that will help you identify this entry or provide details as to why it was added.
Enabled	When this field is checked, the entry will be whitelisted. If unchecked, the entry will be filtered normally.

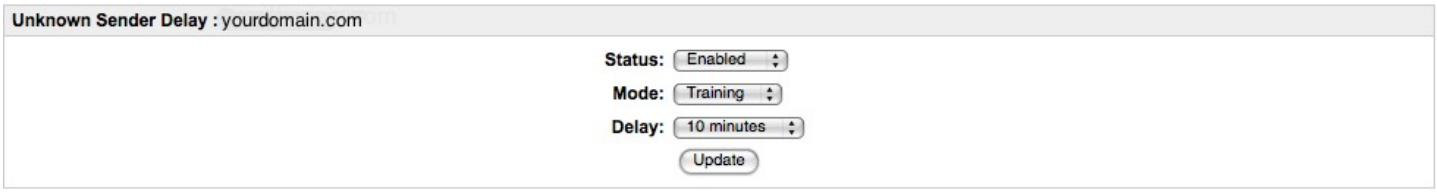
Uploading a List of entries
To upload a text file containing a list of entries, click on the "Upload Whitelist" button. When uploading a list, the list must contain a listing of one IP address or address group, domain or email address per line.

Editing an Entry
To edit an entry, click on the "edit" link in the corresponding row within the main listing.

Enable or Disable an Entry
To enable or disable an entry or group of entries, from the main listing screen, check the checkbox next to each entry you wish to change. Next, select either enable or disable from the drop down list located at the lower left of the list. Finally, click on "Go".

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Unknown Sender Delay



Unknown Sender Delay is a method of handling email from new senders that can greatly help cut down spam. This process works by putting any email from an address that has never sent mail to that MailFoundry appliance before to be delayed by a configurable period of time. This allows the appliance more time to get updated spam rules that may match the incoming spam message.

To use this feature we recommend enabling it in training mode for 3 to 5 days. In that time it starts building a list of addresses that normally send email to the appliance. After that time period it can be changed to delay mode.

After a sender has been added to the Unknown Sender Delay database, future emails received from that sender are not subjected to delay.

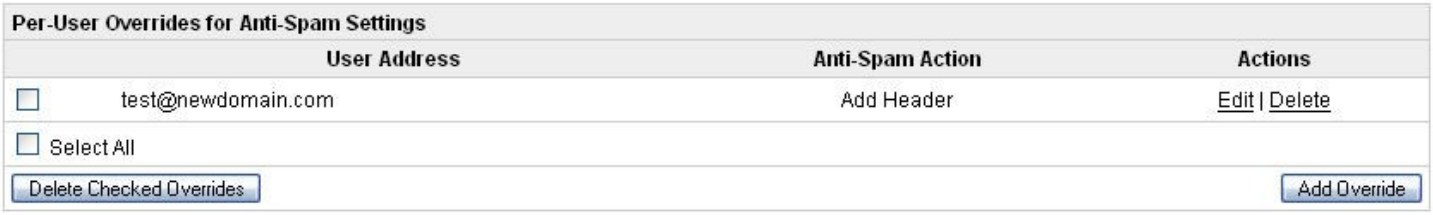
Anti-Spam Settings

This screen allows you to configure your anti-spam options. Settings configured on this screen are domain specific in scope.

Configuring Options
To modify your anti-spam settings, edit the following fields and click on "Update". It is important to remember that these settings will only affect the selected domain.

Field	Description
Anti-Spam Check	This option will allow you to enable or disable anti-spam filtering for your entire system.
Anti-Spam Action	There are several options for defining how detected spam messages are handled. Add "X-MailFoundry: Spam" Header – This option will place a header within the message that can be used for filtering with an email client such as Microsoft Outlook. Redirect spam messages to e-mail address – This option will send all detected spam messages to an email address you define. Tag Subject line with – This option will add a tag at the beginning of the subject line of all detected spam (Example: [SPAM]). Quarantine Message – This option will place the message into Quarantine system. Delete Message – This option will delete all detected spam without notification.

Per-User Overrides



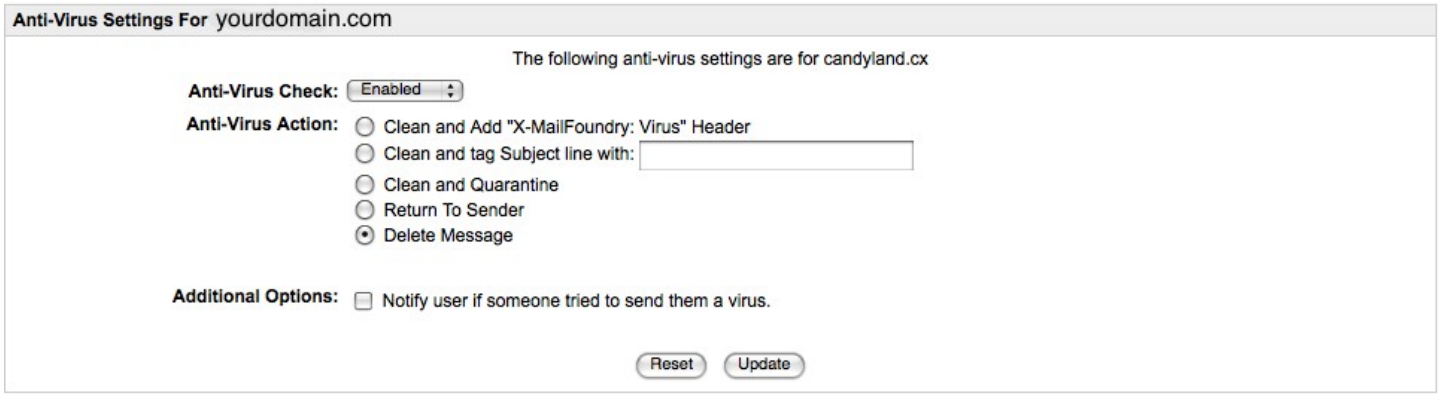
Using the per-user override system, you can configure specific users, by email address, to have different anti-spam setting then the defaults. To add a new override, click on the "Add Override" button in the lower right of the main view.

You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

Editing a Per-User Override
To edit a per-user override, click on the "edit" link in the corresponding row within the main listing.

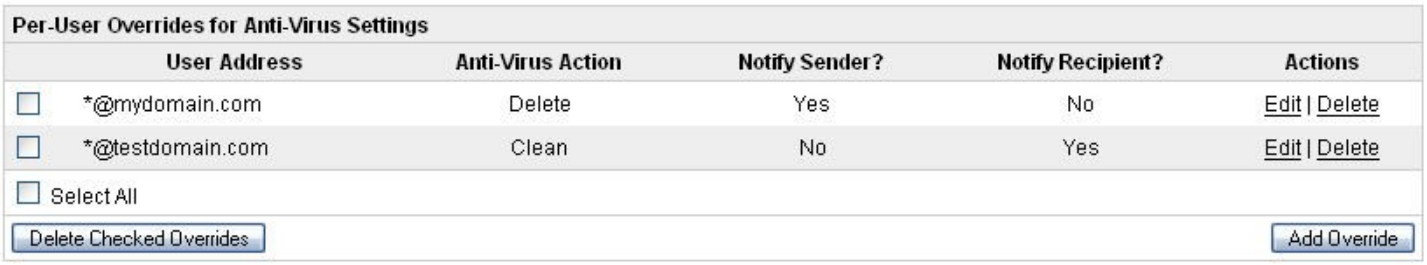
Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides".

Anti-Virus Settings



Field	Description
Anti-Virus Check	This option will allow you to enable or disable anti-virus filtering for your entire system.
Anti-Virus Action	There are several options for defining how detected virus infected messages are handled. Clean and add "X-MailFoundry: Virus" header – This option will clean the infected message and place a header within the message will can be used for filtering with an email client such as Microsoft Outlook. Clean and tag subject line with – This option will clean the infected message and add a tag at the beginning of the subject line of the cleaned message (Example: [VIRUS]). Clean and Quarantine Message – This option will clean the infected message and place the message into quarantine system. Return To Sender – This option will return the infected message back to the sender. Delete Message – This option will delete all infected messages without notification.
Notify User	This option will send a notification message to the recipient of the virus-infected message.

Per-User Overrides



*NOTE: wildcards can not be used.

Using the per-user override system, you can configure specific users, by email address, to have different anti-virus setting than the defaults. To add a new override, click on the "Add Override" button in the lower right of the main view.

You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

Editing a Per-User Override
To edit a per-user override, click on the "Edit" link in the corresponding row within the main listing.

Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides".

Domain Filters

MailFoundry includes a full featured custom filters system. Using custom filters, you can create filters based on content of inbound and outbound messages. Filters created in this section will have a domain specific scope.

Creating a Domain Filter
For details on the context of custom filters, see Chapter 5 – Custom Filters. To create a new custom filter, click on "Add a Filter". Next, enter all required fields and finally, click on "Create Filter".

Editing a Domain Filter
To edit a filter, click on the "Edit" link in the corresponding row within the main listing.

Enable, Disable or Delete a Domain Filter
To enable, disable or delete a filter or group of filters, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Changing a Domain Filters Priority
To change the priority of a custom filter, click either on the "Up" arrow or "Down" arrow in for the custom filter on the main view screen.

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Using Keyword Lists
Your MailFoundry appliance has the ability to filter messages based on a list of keywords you enter or upload. Keyword filtering is effective in blocking message based on the content however using this system can create false-positive detections.

Once you have created your keyword list, you will need to create a custom filter that will utilize the keyword list.

Manually Entering a Keyword List
To manually enter a keyword list, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: "badwords"). Now, enter the keywords in the keyword list field, one per line. When completed, click on "Create".

Uploading a Keyword List
To upload a previously created list of keywords, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: "badwords"). Now, click on the "Browse" button. A directory listing will be displayed that will allow you to locate the saved file on your computers disk drive. Make sure the saved file lists the keywords, one per line. Once you have selected the file, click on "Create". Your file will be uploaded and your keyword list will be created.

Deleting a Keyword List
To delete a keyword list or group of keyword lists, click on the checkbox next to the entries you would like to remove. Next, click on "Delete selected keyword lists".

Address Filters

MailFoundry includes a full featured custom filters system. Using custom filters, you can create filters based on content of inbound and outbound messages. Filters created in this section will have an address specific scope.

Creating an Address Filter
For details on the context of custom filters, see Chapter 5 – Custom Filters. To create a new custom filter, click on "Add a Filter". Next, enter all required fields and finally, click on "Create Filter".

Editing an Address Filter
To edit an address filter, click on the "Edit" link in the corresponding row within the main listing.

Enable, Disable or Delete an Address Filter
To enable, disable or delete a filter or group of filters, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Changing an Address Filters Priority
To change the priority of a custom filter, click either on the "Up" arrow or "Down" arrow in for the custom filter on the main view screen.

View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Using Keyword Lists
Your MailFoundry appliance has the ability to filter messages based on a list of keywords you enter or upload. Keyword filtering is effective in blocking message based on the content however using this system can create false-positive detections.

Once you have created your keyword list, you will need to create a custom filter that will utilize the keyword list.

Manually Entering a Keyword List
To manually enter a keyword list, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: "badwords"). Now, enter the keywords in the keyword list field, one per line. When completed, click on "Create".

Uploading a Keyword List
To upload a previously created list of keywords, click on "Add Keyword List" from the main view screen. Next, enter an internal name for the list (Example: "badwords"). Now, click on the "Browse" button. A directory listing will be displayed that will allow you to locate the saved file on your computers disk drive. Make sure the saved file lists the keywords, one per line. Once you have selected the file, click on "Create". Your file will be uploaded and your keyword list will be created.

Deleting a Keyword List
To delete a keyword list or group of keyword lists, click on the checkbox next to the entries you would like to remove. Next, click on "Delete selected keyword lists".

Quarantine Options

Your MailFoundry appliance includes a full featured quarantine system. Although it is rare to have a false-positive message, using the quarantine system will give your email users the ability to view detected spam messages. You may also choose to have cleaned, virus-infected messages included in the quarantine system. Another unique feature your MailFoundry appliance offers is the ability to quarantine messages based on custom filters.

Configuring Options
To modify your quarantine settings, edit the following fields and click on "Update". Settings modified in this section are domain specific in scope.

Field	Description
Quarantine Queue Lifespan	This option will allow you to set the number of days messages will remain active in the quarantine system between one and 45 days.
Quarantine Digest Format	This option will allow you to set the format of the quarantine digest messages mailed to your email users.
Quarantine Digest Frequency	This option will allow you to define the frequency of which digest messages are sent to users. You may choose to send the digests once per hour, once per day including weekends, or once per day excluding weekends.
Message to be included in the user digest notifications	This option will allow you to define a custom message which will be included with the digest messages. You may include the following HTML tags for formatting: <b> <i> <p> <u> <img> <a> <font> <table> <tr> <td>

Per-User Overrides

Using the per-user override system, you can configure specific users, by email address, to have different quarantine setting than the defaults.

To add a new override, click on the "Add Override" button in the lower right of the "Overrides for Quarantine Settings" box.

You will need to enter the users email address and then define their customized settings. Once completed, click on "Add Override" to save.

Editing a Per-User Override
To edit a per-user override, click on the "Edit" link in the corresponding row within the main listing.

Deleting Per-User Overrides
To delete per-user overrides, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Checked Overrides" in the lower left of the "Overrides for Quarantine Settings" box.

Digest Redirections

A digest redirection allows you to redirect the digest messages for a specific email address to another email address. This is often beneficial when you have an alias which multiple users answer and you only need one person who is a member of the alias to manage the quarantine digests.

To add a new redirection, click on the "Add a Digest Redirection" button in the lower right of the "Digest" box.

Enter the email address that you would like to redirect digest messages for. Next, enter the destination email address who will manage the quarantine for the redirected address. Finally, click on "Add Digest Redirection" to save you entry.

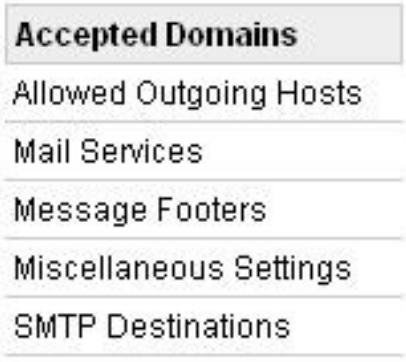
Editing a Digest Redirection
To edit a digest redirection, click on the "Edit" link in the corresponding row within the main listing.

Deleting Digest Redirections
To delete digest redirections, click on the checkbox next to the entries you would like to remove. Next, click on "Delete Selected Digest Redirections" in the lower left of the "Digest Redirections" box.

SMTP Settings Tab – System Level

SMTP, short for Simple Mail Transfer Protocol, is the protocol used by email servers to communicate and transfer messages. Settings found in this section are related to sending, receiving, processing and formatting of messages.

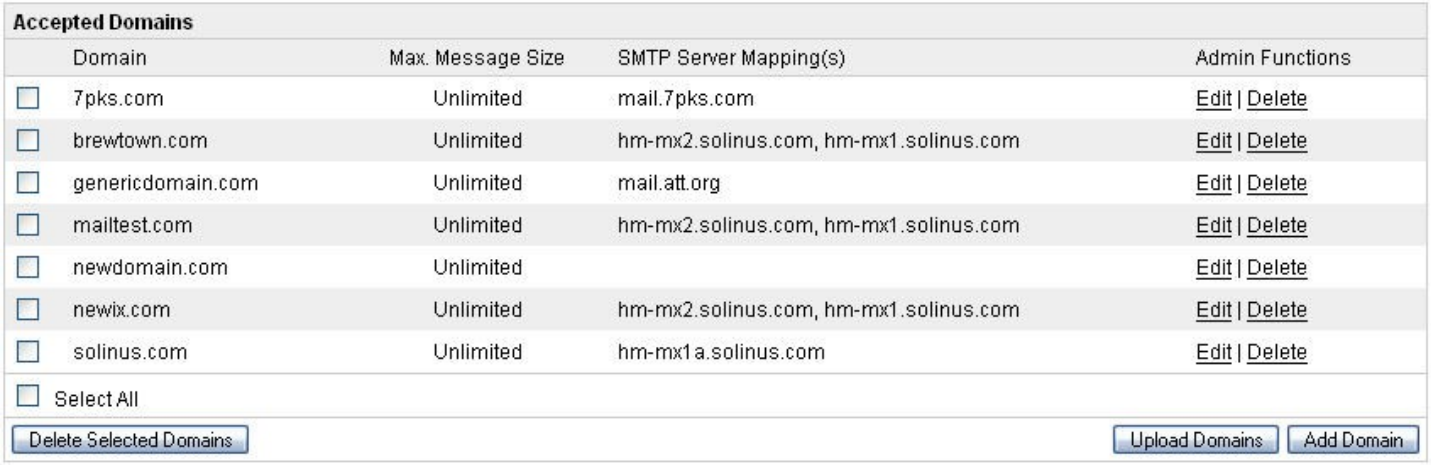
Configurations set in this section are system wide in scope and can be overridden using a domain specific setting.



Menu Structure	
Accepted Domains	This option allows you to add, edit and delete accepted domains that will be filtered by your MailFoundry appliance.
Allowed Outgoing Hosts	This option allows you to define which hosts may send outbound messages through your MailFoundry appliance.
Mail Services	This option allows you to stop, start or restart the Mail Service on your MailFoundry appliance.
Message Footers	This option allows you to define text messages that can be appended to incoming, outgoing and internal messages.
Miscellaneous Settings	This option allows you to configure miscellaneous options including the default domain and auto-domain system.
SMTP Destinations	This option allows you to configure SMTP Destination Servers.

Accepted Domains
Each domain that will be processed by the MailFoundry appliance will need to be added to the Accepted Domains list if you are not using the Auto Domains feature. Using this system, you can configure domain specific options such as the maximum message size and anti-virus services.

SMTP server mapping is also done within the Accepted Domains screen. Domains may target one or more SMTP servers.



Adding a New Entry
To add a new entry to the Accepted Domains system, click on the "Add Domain" button. Fill in the fields as listed below

Field	Description
New Domain	Enter the domain name you would like to process messages for (Example: mydomain.com).
Maximum Message Size	Select the maximum message size you wish to accept for processing. This field should match the maximum message size allowed by your target SMTP server.
Virus Protection	Select "Enable" to have messages addressed to this domain scanned for virus infections.

Next, you will be asked to select one or more destination SMTP servers that will receive messages for the domain. Check the checkbox in the corresponding rows for those servers which you would like to map to the domain. You may optionally change the following settings for each destination SMTP server:

Field	Description
Priority	Select the priority for this server. If selecting multiple servers you may have them at equal priority to load balance message traffic.
Port	Select the TCP/IP port your SMTP destination server is configured to use for inbound message traffic.

Once you have selected all of the servers you wish to map for the domain, click on the "Update" button.

Adding A New Destination SMTP Server
You may choose to add a new destination SMTP server from this screen. To do so, check the checkbox in the last row of the domain mapping list. Next, enter the hostname or IP address of the new server. Select the priority for the server and finally, configure the TCP/IP port to be used and click on the "Update" button.

Uploading a List of entries
To upload a text file containing a list of entries, click on the "Upload Domains" button. When uploading a list, the list must contain a listing of one domain name per line. Optional you can add additional configurations options in the following format:

Domain.com, SMTP_SERVER, Virus Protection, Max_Message_Size_in_MB

The "Virus Protection" field can either be set to 'Enabled' or 'Disabled'.

The "Max_Message_Size_in_MB" is the maximum size in megabytes that you will accept for the particular domain. For unlimited size, enter 0.

Searching a Domain
To search for a listed domain, enter the full domain name or a portion of the domain name into the "Search for a domain" text field in the "Search" section and click on "Search".

Editing a Domain
To edit a domain, click on the "Edit" link in the corresponding row within the main listing.

Enable or Disable a Domain
To enable or disable a domain or group of domains, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable or disable from the drop down list located at the lower left of the list. Finally, click on "Go".

Allowed Outgoing Hosts

Field	Description
Address or Space	Enter the IP Address or IP address block in the following format: 192.168.0.1
Address Type	Select the address type of either a single IP address, an address blocked with a bit mask (Example: /24) or an address block with a subnet mask (Example: 255.255.255.0).
Enabled	When this field is checked, the entry will be enabled and able to send outgoing messages through your MailFoundry appliance. If unchecked, the entry will be disabled.
Notes	You can enter an internal description that will help you identify this entry or provide details as to why it was added.

Uploading a List of Entries
To upload a text file containing a list of entries, click on the "Upload List" button. When uploading a list, the list must contain a listing of one IP address per line.

Searching an IP Address
To search for a listed IP address, enter the IP Address into the "Search for an IP" text field in the "Search" section and click on "Search".

Editing an IP Address
To edit an Address, click on the "Edit" link in the corresponding row within the main listing.

Enable, Disable or Delete an IP Address
To enable, disable or delete an IP address or group of IP addresses, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

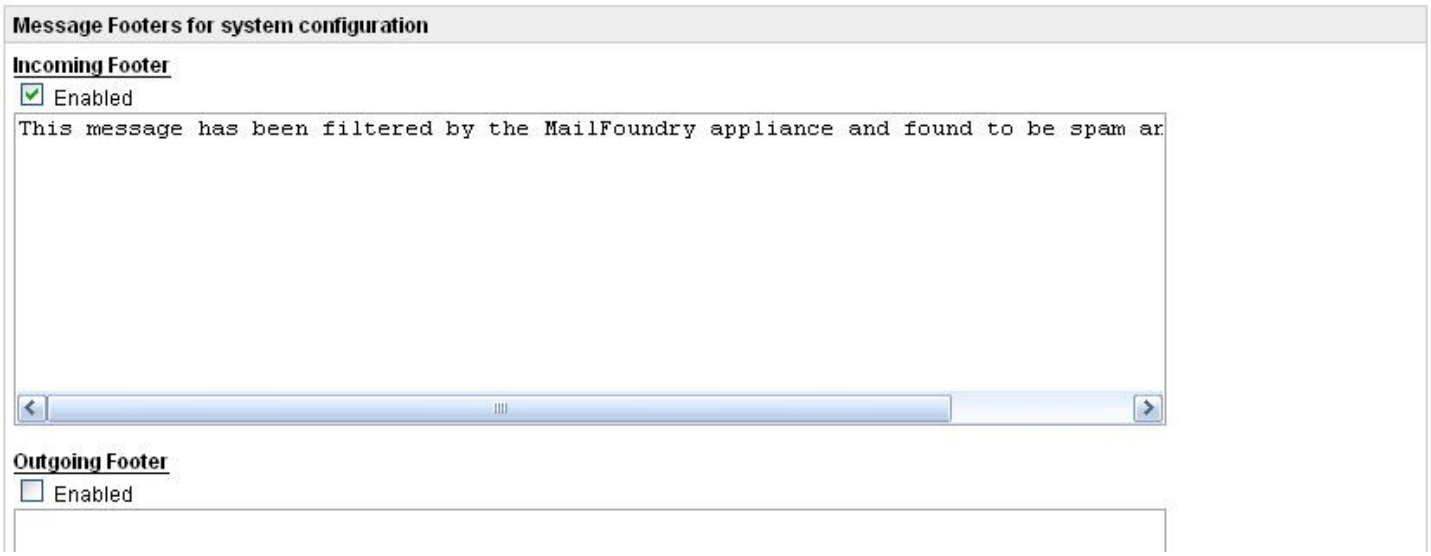
View Usage Statistics
To view usage statistics, click on the "Show Stats" link near the bottom on the left side of the main listing display. To hide usage statistics, click on "Hide Stats".

Mail Services

This screen allows you to manage your MailFoundry Appliance's mail services. You can stop, restart or start the service as needed.

When the mail service is disabled, messages will not be received or processed by your MailFoundry appliance.

Message Footers


Message Footers for system configuration
Incoming Footer
Enabled
This message has been filtered by the MailFoundry appliance and found to be spam ar
Outgoing Footer
Enabled

Message footers are text messages that are added at the end of incoming, outgoing or internal messages. This makes the message multipart.

Incoming messages are messages from the internet which are destined for a local user.

Outgoing messages are messages created from a local user destined for a user over the internet.

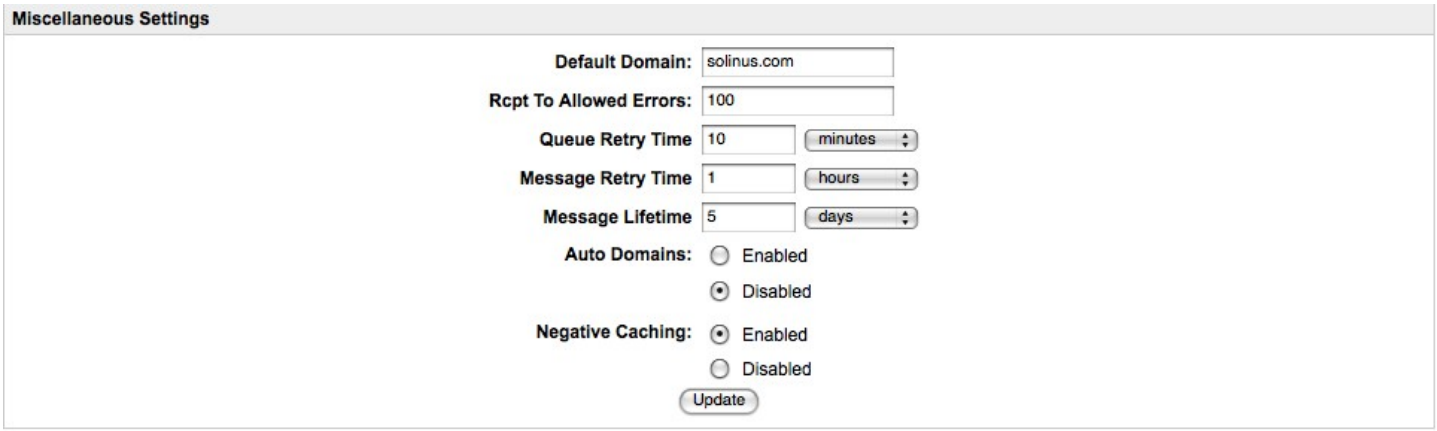
Internal messages are messages created by a local user destined for another local user.

Enabling Message Footers
To enable a message footer enter the text you wish to include and check the "Enable" checkbox for each footer type you wish to use. Next, click on the "Update" button at the bottom of the page.

Disabling Message Footers
To disable a message footer, uncheck the "Enable" checkbox for each of the footers you wish to disable. Next, click on the "Update" button at the bottom of the page.

Miscellaneous Settings

This section allows you to configure the default domain used by the MailFoundry appliance. You can also enable or disable the "Auto Domains" feature here.



Default Domain
The default domain option allows you to define a domain to be assigned to messages destined to 'postmaster' where a domain has not been defined. A default domain should be created when you have multiple domains processed by your MailFoundry appliance.

RCPT To Allowed Errors
Rcpt To Allowed Errors, is a setting that allows you to adjust how many bad addresses can be attempted in a single incoming SMTP connection before that connection is dropped. This can be used to block certain kinds of spam attacks if a single connection is used to try to send to a large quantity of bad email addresses.

The Redlisting feature uses similar information in a more complete way.

Queue Retry Time
The Queue Retry Time represents how often each queue (incoming, outgoing, and unscanned) is processed to see which messages need to be retried. Default is 10 minutes (600 seconds).

Message Retry Time
The Message Retry Time is how long a message will stay in its queue before being retried. Default is one hour (3600 seconds).

Message Lifetime
The Message Lifetime is the amount of time a message will stay in the queue before it is considered undeliverable, and deleted. Default is 5 days (432000 seconds).

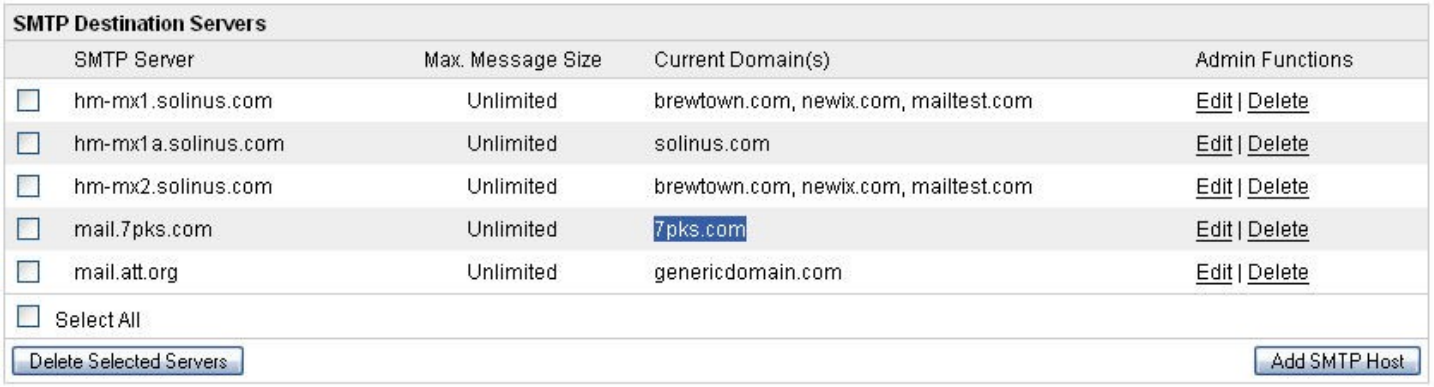
Auto Domains
Auto Domains, is a unique feature included with your MailFoundry appliance that makes management of systems with large amounts of domains very easy. With Auto Domains, it is not necessary to provision and manage individual domains. Your MailFoundry appliance will automatically detect new domains and provision them as needed.

Once this service is enabled, any new inbound connection will be verified, using the SMTP protocol, with each previously configured SMTP destination servers. Auto Domains will check each SMTP destination server to see if it accepts messages for the newly detected domain. If one or more SMTP destination servers are verified for the newly detected domain, the domain will be provisioned and each verified SMTP destination server will be added to the domain's SMTP mapping list.

It may take up to 10 days for the MailFoundry appliance to remove an automatically provisioned domain name if it is removed from the SMTP destination server(s). It is recommended that you manually delete the domain from your MailFoundry appliance once the domain's MX record change has fully propagated

Negative Caching
Negative caching allows the MailFoundry server to cache negative responses from your backend SMTP server for invalid addresses, for up to 30 minutes. This will enable the MailFoundry server to automatically reject mail for invalid addresses without checking with the backend server. However, if you have extra filtering on the backend server that can give permanent errors for valid addresses, you will want to turn this feature off.

SMTP Destinations



SMTP Destinations are SMTP servers that your MailFoundry appliance will route messages to. MailFoundry will work with SMTP compliant mail servers including Microsoft Exchange, Sendmail, Qmail, Postfix, Merak and others.

Each domain you process messages for requires at least one SMTP destination although you may configure as many SMTP destinations as needed.

Adding a New Entry
To add a new SMTP destination, click on the "Add SMTP Host" button. Fill in the fields as listed below

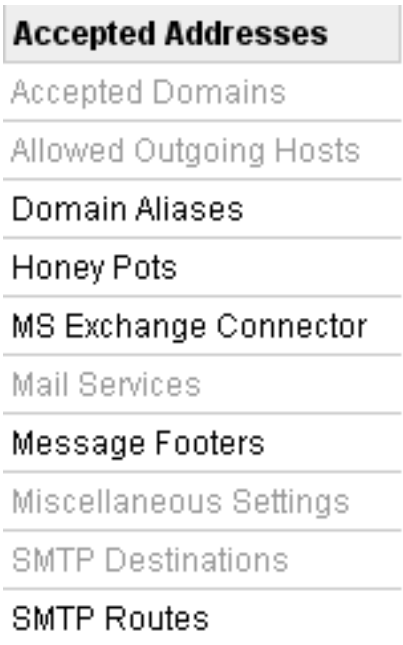
Field	Description
New SMTP Server	Enter the host name and domain name of your SMTP server (Example: mail.mydomain.com).
Default Port	Select the default TCP/IP port your SMTP destination server is configured to use for inbound message traffic. This can be modified on a per-domain basis.
Default Priority	Select the default priority for this server. This can be modified on a per-domain basis.
Maximum Message Size	Select the maximum message size you wish to accept for processing. This field should match the maximum message size allowed by your target SMTP server.

Searching an SMTP Destination
To search for a listed SMTP Destination Server, enter the full or partial host name into the "Search for a server name" text field in the "Search" section and click on "Search".

Editing an Entry
To edit an entry, click on the "edit" link in the corresponding row within the main listing.

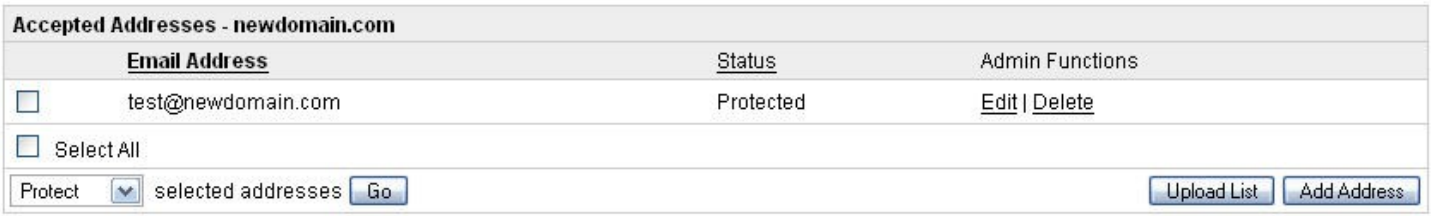
Enable, Disable or Delete an Address
To enable, disable or delete an IP address or group of IP addresses, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

SMTP Settings – Domain Level



Accepted Addresses	This option allows you to define a list of email address which will be protected or unprotected from spam and viruses.
Domain Aliases	This option allows you to define a list of additional domains that will have the same user mappings as the parent domain.
Honey Pots	This option allows you to add addresses that will auto forward emails to the spam feed.
MS Exchange Connector	This option allows you to configure the Microsoft Exchange Connector service. This service will validate email address using a special LDAP connection to your Exchange Server.
Message Footers	This option allows you to define text messages that can be appended to incoming, outgoing and internal messages.
SMTP Routes	This option allows you to configure mapping for this domain to a list of destination servers.

Accepted Addresses



The Accepted Addresses list allows you to control which addresses for a given domain are processed. In addition, you can define how email addresses that are not listed are handled.

By default, the MailFoundry appliance will process all messages as long as your destination SMTP server authenticates the email address.

Some SMTP servers however do not process SMTP authentication request as required by MailFoundry. In these cases, any possible email address would be considered valid unless limited by the Accepted Addresses system.

Auto Discover Email Addresses

When this option is enabled, new email addresses that receive inbound messages and are not currently listed in the Accepted Addresses list will be "Auto Discovered". Messages for these addresses will be forwarded to your destination SMTP server. If you have selected the "Check unlisted email addresses for Spam / Virus" checkbox, these messages will be processed for spam and viruses.

Adding a New Entry

To add a new entry to the Accepted Addresses list, click on the "Add Address" button. Fill in the fields as listed below

Field	Description
E-mail Address	Enter the email address you wish to define as protected or unprotected.
Status	Select either "Protected", which tells MailFoundry to process messages to this user for spam and viruses, or "Unprotected" which means all messages are past directly to your destination server without filtering.

Uploading a List of Entries

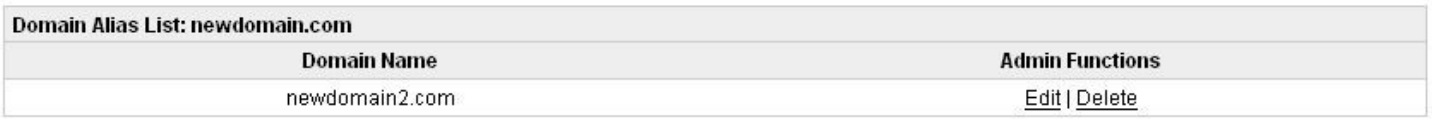
To upload a text file containing a list of entries, click on the "Upload List" button. "When uploading a list, the list must contain a listing of one email address per line". You must specify by using the "Status" checkbox if the address list is "Protected" or "Unprotected".

Searching an Email Address
To search for a listed email address, enter the email Address into the "Search for an address" text field in the "Search" section and click on "Search".

Editing an Email Address
To edit an email address, click on the "edit" link in the corresponding row within the main listing.

Protect, Unprotect or Delete an Email Address
To Protect, Unprotect, or delete an email address or group of email addresses, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either protect, unprotect or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Domain Aliases



Domain Aliases allow you to configure secondary domain names which mirror the configuration of the primary domain.

Support for domain aliases is dependent on your destination SMTP server. Your MailFoundry appliance will process messages for the secondary domain using the exact configurations of the primary domain. If you need a variation in configuration for the secondary domain, it is recommended that you configure the secondary domain as a separate domain within your MailFoundry appliance.

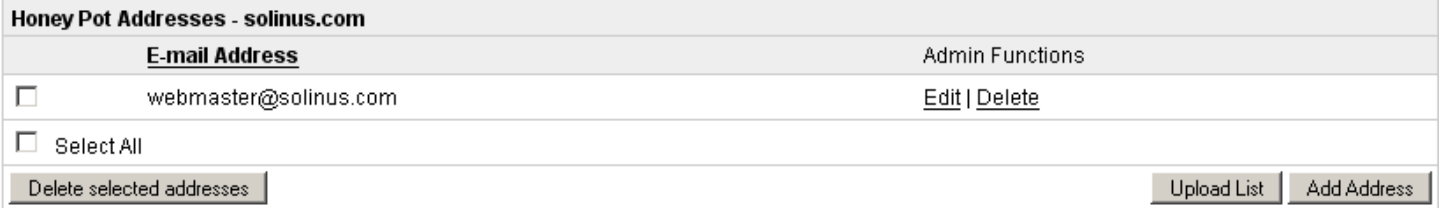
Adding a Domain Alias
To add a domain alias, enter the full domain name of the secondary domain name in the "New Domain Alias" field. Next, click on "Add".

Editing a Domain Alias
To edit a domain alias, click on the "Edit" link in the corresponding listing row.

Deleting a Domain Alias
To delete a listed domain alias, click on the "Delete" link in the corresponding listing row.

Honey Pots

Honey pots are addresses that automatically forward all email sent to them to spam@mailfoundry.com. To use honey pots it's best to add email addresses that have never existed on the domain before. This way any email going to it will be a phishing attempt and needs to be forwarded to spam@mailfoundry.com.

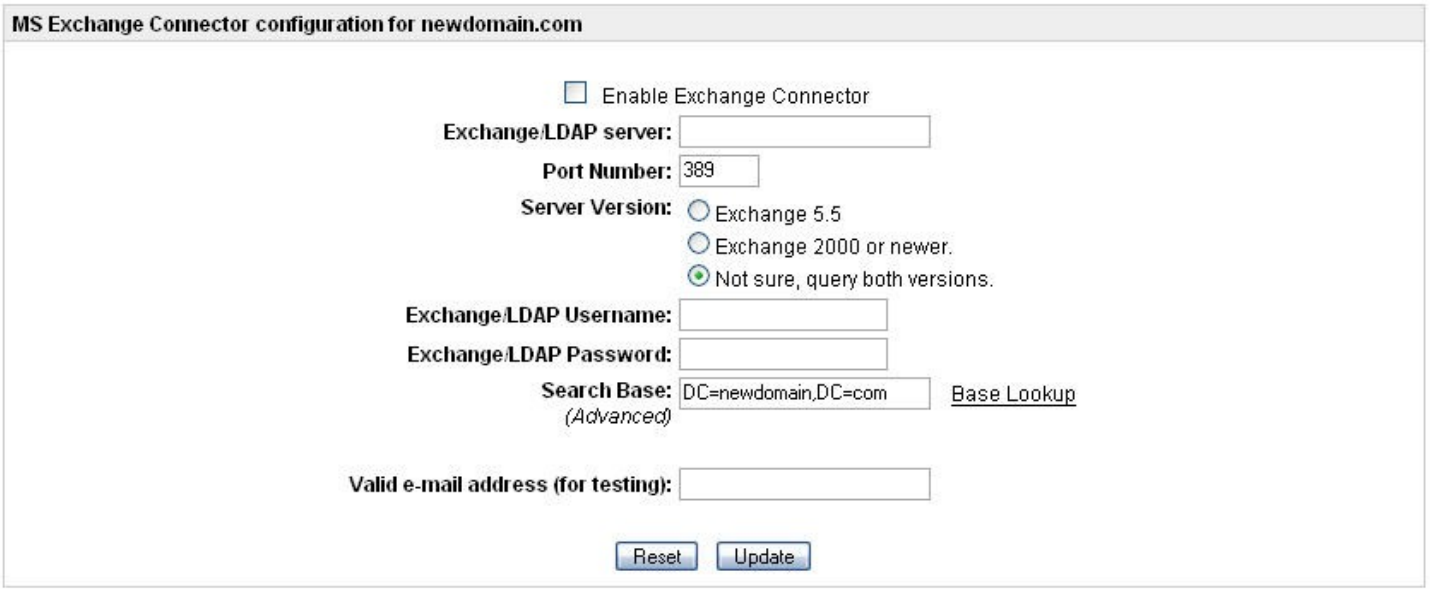


Adding a Honey Pot
To add a honey pot, Click the *Add Address* button, then enter the address you wish to use as a Honey Pot. Click Add to add this address to the Honey Pots.

Editing a Honey Pot
To edit a Honey Pot, click on the "Edit" link in the corresponding listing row.

Deleting a Domain Alias
To delete a listed Honey Pot, click on the "Delete" link in the corresponding listing row.

MS Exchange Connector



The MS Exchange Connector is a specialized LDAP connection between your MailFoundry appliance and your Exchange server for the purpose of account address verification.

Because Microsoft Exchange does not support SMTP based user authentication, it is highly recommended that the MS Exchange Connector be used with all Microsoft Exchange installations. If this option is not used, every possible email address will be considered valid which could cause your MailFoundry appliance to become unstable.

Configuring Options
To modify your MS Exchange Connector settings, edit the following fields and click on "Update". It is important to remember that settings are domain specific.

Field	Description
Enable Exchange Connector	Click on this checkbox in order to enable the MS Exchange Connector for this domain.
Exchange/LDAP server	Enter the full address of your Domain Controller that will answer Exchange/LDAP queries.
Port Number	Enter the TCP/IP port number that your Domain Control answers Exchange/LDAP queries on. The default is 389.
Server Version	Select either "Exchange 5.5" or "Exchange 2000" or newer. If you are unsure, you can select "Not sure, query both versions".
Exchange/LDAP Username	Enter the user name which will be used to authenticate with your Domain Controller. If you are using anonymous authentication, leave this filed blank.
Exchange/LDAP Password	Enter the password which will be used to authenticate with your Domain Controller. If you are using anonymous authentication, leave this filed blank.
Search Base	For Advanced users Only – The default option should work for most installations.
Valid e-mail address (for testing	Enter a valid email address which should be authenticated by your Domain Controller. This is used to test your settings and verify that the connection has been made successfully.

Message Footers

Message footers are text messages that are added at the end of incoming, outgoing or internal messages.

Internal messages are messages from the internet which are destined for a local user.

External messages are messages created from a local user destined for a user over the internet.

Internal messages are messages created by a local user destined for another local user.

Adding footers causes emails to become multipart messages. Some email clients may not display this information correctly.

SMTP Routes

Adding a New Entry
To add a new entry to the Allowed Outgoing Hosts system, complete the files on the last listing row as listed below. Next, click on the "Update" button.

Field	Description

New SMTP Server	Enter the host name and domain name of your SMTP server (Example: mail.mydomain.com).
Port	Select the TCP/IP port your SMTP destination server is configured to use for inbound message traffic.
Priority	Select the priority for this server.

Enable or Disable a SMTP Route

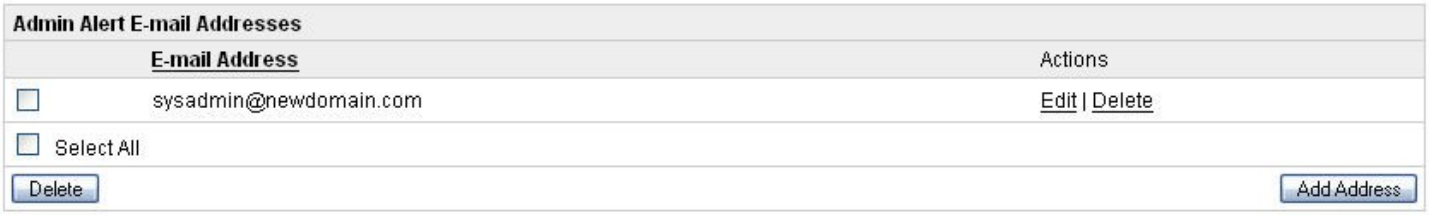
To enable or disable a SMTP Route either check or uncheck the corresponding checkbox next to each listing. Once completed, click on the "Update" button.

System Settings Tab

The System Settings tab provides the ability to configure non-email related functions such as networking configurations security settings and system maintenance.

Menu Structure	
Alert E-mail Addresses	This option allows you to configure a list of email addresses which will be notified if there are technical issues with your MailFoundry appliance.
Branding	This Option allows for customization of the User interfaces logo's
Date & Time Settings	This option allows you to configure various date and time related options.
External Logging	This option allows you to configure external syslog settings.
Login Accounts	This option allows you to configure a list of users who may log into the MailFoundry appliance's user interface.
Login IP Restrictions	This option allows you to configure a list of IP addresses which users with login accounts may access the MailFoundry appliance's user interface.
Maintenance	This option allows you to perform system maintenance.
Network Configuration	This option will display your current network settings. To change these settings you must use the console access port.
Network Troubleshooting	This window contains tools to test internet connectivity from the appliance.
Remote System Backups	This option will allow you to configure the remote backup service included with your MailFoundry subscription.
SSL certificates	This option allows you to setup SSL certificates on the MailFoundry appliance
SSL Settings	This allows you to change the SSL settings and Configurations on the appliance.
Shutdown / Restart	This option will allow you to shutdown or restart your MailFoundry appliance.
Support Admin Login	This option will allow you to enable or disable the remote login support for MailFoundry support staff.
System Status	This option will display current system and hardware status information.
System Updates	This option will allow you to switch from automatic system updates to manual updates. If manual updates are selected, you can install updates manually from this section.
Technical Contact List	This option will allow you to create a list of email addresses that will receive technical update notifications from MailFoundry support staff.

Alert E-mail Addresses



Addresses added to this list will receive automated notifications from the MailFoundry appliance if a technical issue is detected. This can include such things as disk usage being at a critical state. It is recommended that you have all system administrators added to this list.

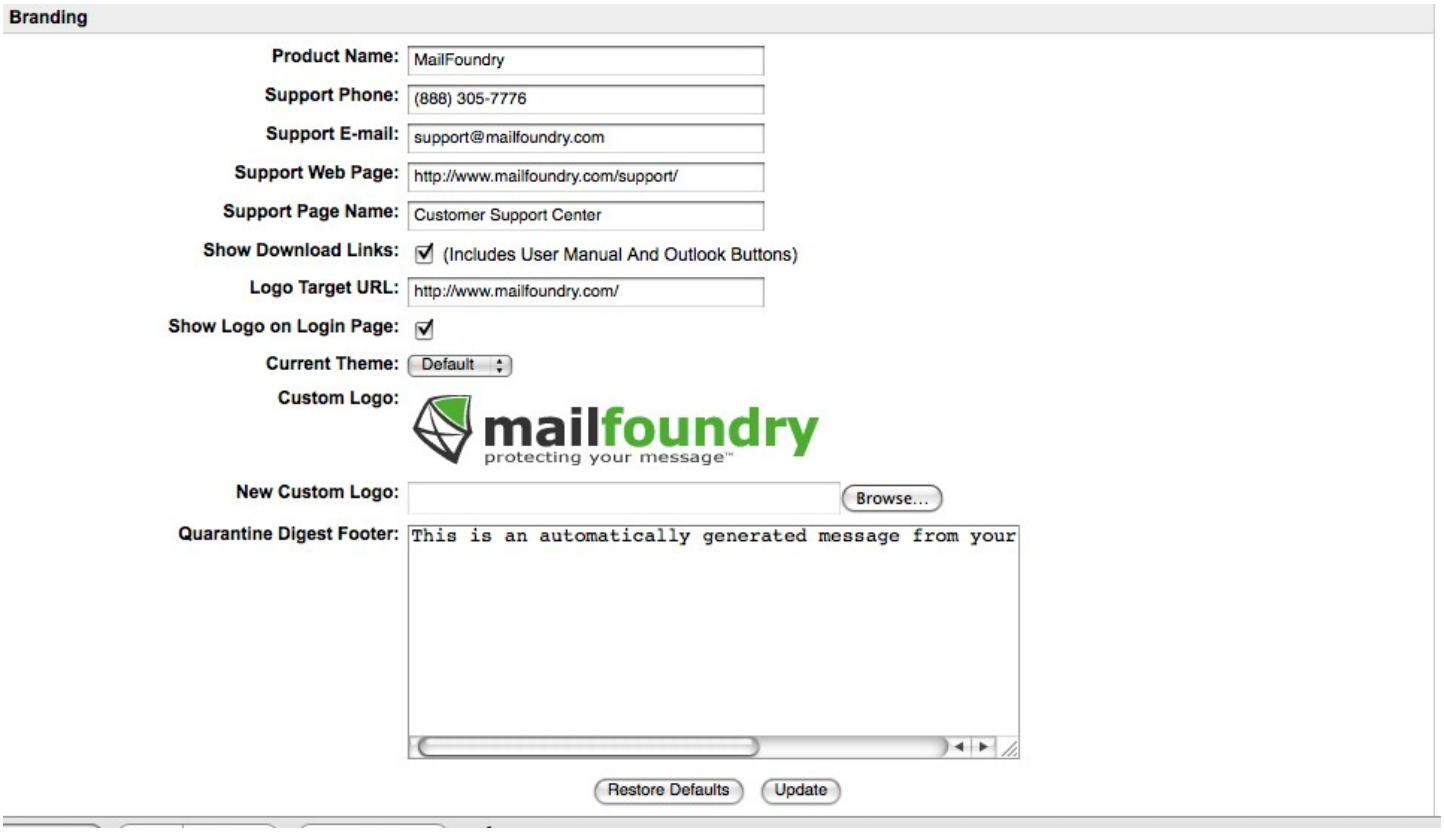
Adding a New Address
To add a new entry to the Alert E-mail Addresses list, click on the "Add Address" button. Next, enter the full email of the user. Finally, click on the "Add" button.

Editing an Address
To edit an address, click on the "edit" link in the corresponding row within the main listing.

Deleting an Address

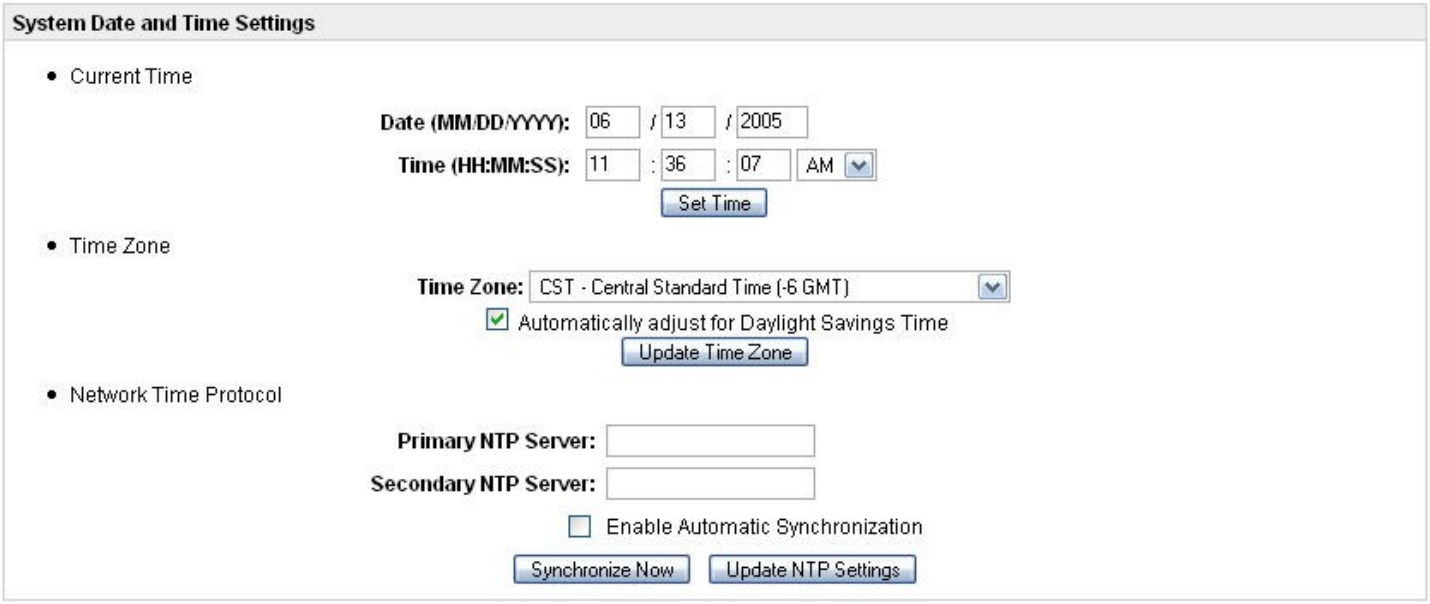
To delete an address from the alert E-mail Address list, check the corresponding checkbox next to each listing you wish to delete. Next, click on the "Delete" button.

Branding



Branding allows customers to brand the appliance's GUI with a custom logo and contact information. This is usually done in order to avoid confusion with end users. All variables set here will update all values across the appliance's feature set, including the branding of the quarantine digest messages.

Date and Time Settings


System Date and Time Settings
Current Time
Date (MM/DD/YYYY): 06 / 13 / 2005
Time (HH:MM:SS): 11 : 36 : 07 AM
Set Time
Time Zone
Time Zone: CST - Central Standard Time (-6 GMT)
Automatically adjust for Daylight Savings Time
Update Time Zone
Network Time Protocol
Primary NTP Server:
Secondary NTP Server:
Enable Automatic Synchronization
Synchronize Now
Update NTP Settings

Field	Description
Date (MM/DD/YYYY)	Enter the current date in the MM/DD/YYY format (Example 11/04/2004)
Time (HH:MM:SS)	Enter the current time in the HH:MM:SS format (Example: 12:00:00). Make sure to set the AM or PM option correctly.

Configuring Your Time Zone
To modify your Time Zone settings, edit the following fields and click on the "Update Time Zone" button.

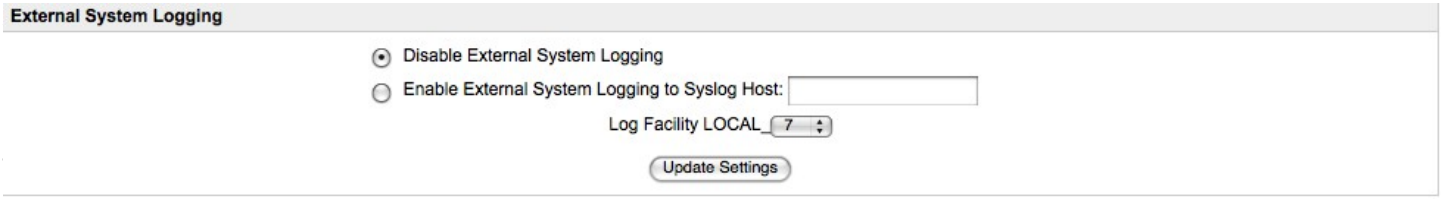
Field	Description
Time Zone	Select your time zone for the list provided.
Automatically adjust for Daylight Savings Time	Check this option if you time zone observes Daylight Savings Time.

Configuring Network Time Protocol
To modify your Network Time Protocol (NTP) settings, edit the following fields and click on the "Update NTP Settings" button.

Field	Description
Primary NTP Server	Enter the address of your primary NTP server.
Secondary NTP Server	Enter the address of your secondary NTP server.
Enable Automatic Synchronization	When this option is checked, your MailFoundry appliance will automatically update the system time with the time collected from the configured NTP servers.

Manually Synchronize with NTP
To manually synchronize your MailFoundry appliance's system time with the time provided by your NTP server, click on the "Synchronize Now" button.

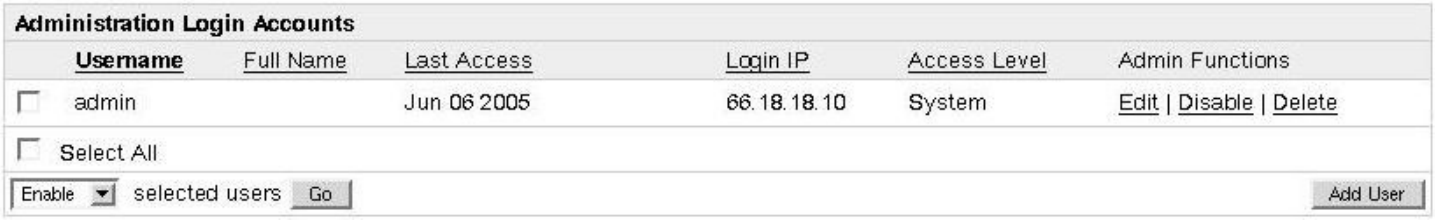
External System Logging


External System Logging
Disable External System Logging
Enable External System Logging to Syslog Host:
Log Facility LOCAL_ 7
Update Settings

Settings" button.

Field	Description
Disable External System Logging	Check this option to disable external system logging.
Enable External Logging to Syslog Host:	Check this option to enable external system logging. You will also need to enter the address or IP address of your syslog server.
Log Facility LOCAL_	Select the Log Facility channel you want to use for your syslog server.

Login Accounts



administer.

Adding a User
To add a new user, click on the "Add User" button. Fill in the fields as listed below

Field	Description
Username	Enter the user name you would like to assign to the new user.
First Name	Enter the first name of the new user.
Last Name	Enter the last name of the new user.
Access Level	Select the access level for the new user. The user may be either a system administrator or a domain administrator.
Password	Enter the password you would like to assign the new user.
Password (again)	Re-enter the password you would like to assign to the new user.

Assigning Domains to Domain Administrators
Once you have created a new user set to the Domain Administrator access level, you can attach their account to the domains they will be able to manage. To do this, click on the "Domains" link within the user listing on the main listing screen.

The MailFoundry appliance will display a list of configured domains on your appliance. Click on the checkbox next to each of the domains this user will have access to.

Next, click on the "Update" button.

Searching for a User
To search for a user, enter the full or partial user name into the "Search for a user" text field in the "Search" section and click on "Search".

Editing a User
To edit a user, click on the "edit" link in the corresponding row within the main listing.

Enable, Disable or Delete a User
To enable, disable or delete a user or group of users, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Login IP Restrictions

For additional security, you may choose to limit the IP addresses which have access to the MailFoundry appliance's user interface. By default, the MailFoundry appliance allows connections for any IP address as long as the user authenticates with the correct user name and password.

It is important to note that it is possible to lock yourself out of your MailFoundry appliance by improperly configuring this option.

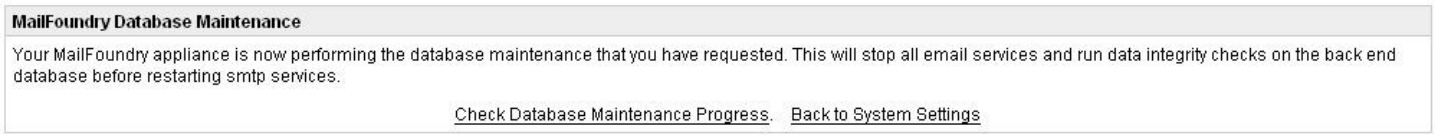
Adding an Allowed IP Addresses
To add a new entry to the Allowed IP Address system, click on the "Add Address" button. Fill in the fields as listed below

Field	Description
Address or Space	Enter the IP Address or IP address block in the following format: 192.168.0.1
Address Type	Select the address type of either a single IP address, an address blocked with a bit mask (Example: /24) or an address block with a subnet mask (Example: 255.255.255.0).
Enabled	When this field is checked, the entry will be enabled and able to send outgoing messages through your MailFoundry appliance. If unchecked, the entry will be disabled.
Notes	You can enter an internal description that will help you identify this entry or provide details as to why it was added.

Editing an Allowed IP Address
To edit an allowed IP address, click on the "edit" link in the corresponding row within the main listing.

Enable, Disable or Delete Allowed IP Addresses
To enable, disable or delete an allowed IP address or group of addresses, from the main listing screen, check the checkbox next to each listing you wish to change. Next, select either enable, disable or delete from the drop down list located at the lower left of the list. Finally, click on "Go".

Maintenance


MailFoundry Database Maintenance
Your MailFoundry appliance is now performing the database maintenance that you have requested. This will stop all email services and run data integrity checks on the back end database before restarting smtp services.
Check Database Maintenance Progress.
Back to System Settings

If in the event that your MailFoundry appliance appears to not be correctly processing messages or you notice issues with your quarantine system, we recommend you perform database maintenance on your appliance.

Many issues can be resolved by using the database maintenance system. You are encouraged to run the database maintenance system before contacting technical.

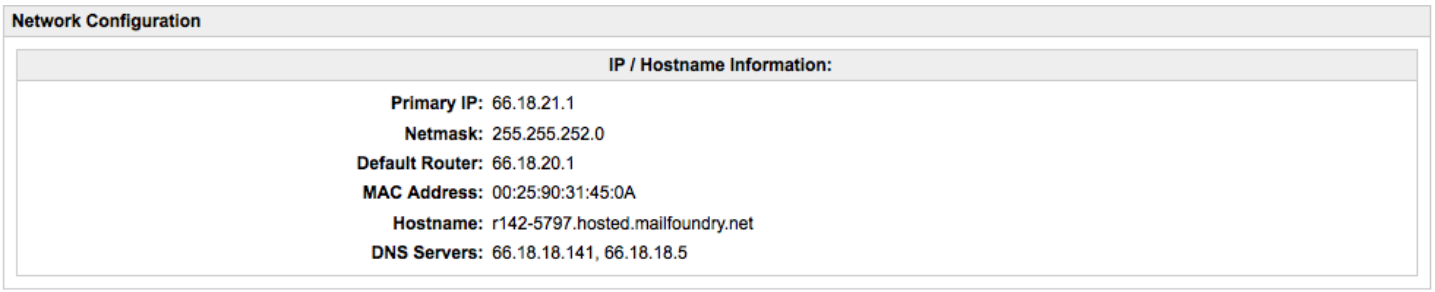
The database maintenance system will stop the mail services, restart the back-end databases, verify the integrity of the database and then restore the mail services.

This process may take several minutes or longer to complete. If you have a very large quarantine, the time to perform this action could exceed one hour.

To perform database maintenance, click on the "Run Database Maintenance" button.

Once the process begins, you can click on the "Check Database Maintenance Progress" link to view the progress of the process.

Network Configuration

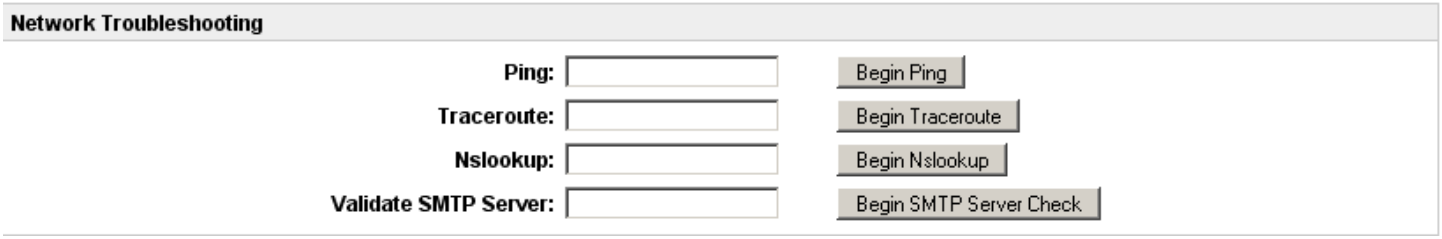


You can view the network settings for MailFoundry here

Making Changes

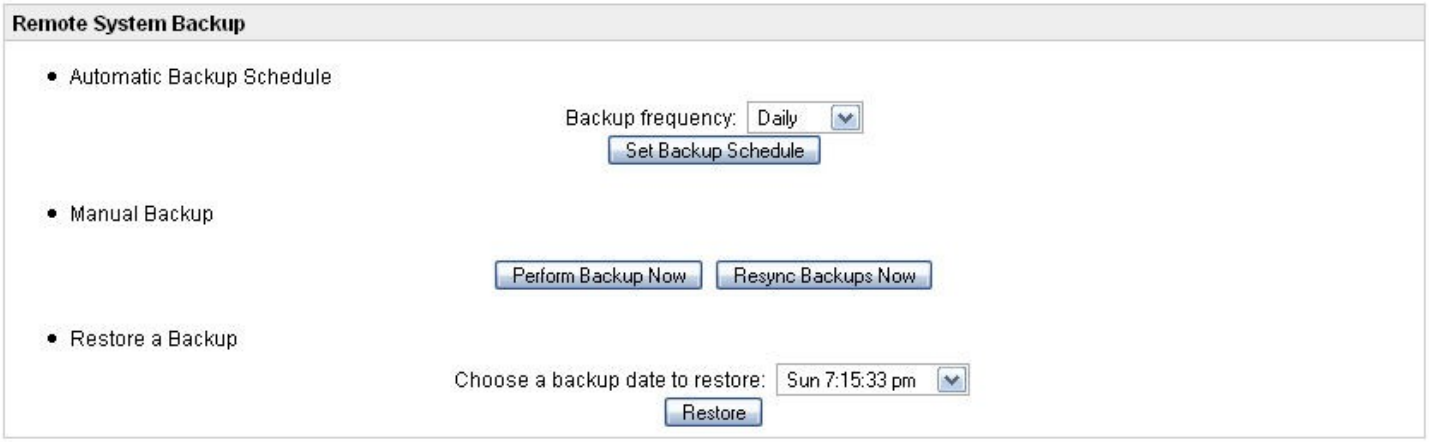
You will not be able to make changes to this information for the Hosted Dedicated service.

Network Troubleshooting



The network troubleshooting are some tools that can be used to try and diagnose internet connectivity issues from the MailFoundry Appliance.

Remote System Backups



Your MailFoundry appliance includes a Remote backup service that securely places your system backups in an off-site location in case of system failure. This service is included as part of your MailFoundry subscription.

Setting an Automatic Backup Schedule
Select the frequency you would like your appliance configurations to be backed up and sent to our remote backup system. Options include daily, weekly or monthly. Next, click on the "Set Backup Schedule" button.

Perform a Manual Backup
If you need to perform a manual backup of your MailFoundry appliance configurations out of schedule, click on the "Perform Backup Now" button.

Re-Synchronize Backups
To re-synchronize your backup list with the stored backups listed in the remote backup server, click on the "Resync Backups" button. Your appliance will verify that all listed backups are in fact stored on the remote backup server. If it us unable to verify a backup set, it will be removed from your available backups listing.

Restore from a Backup
To restore your appliance using a previously backed up configurations set; select the backup from the "Choose a backup date to restore" list. Next, click on the "Restore" button.

SSL Settings

SSL Certificates

The SSL Certificate Generation section allows you to generate a Private Key and a Certificate Signing Request (CSR) that can then be downloaded and used to get a certificate from a Trusted Certificate Authority (CA).

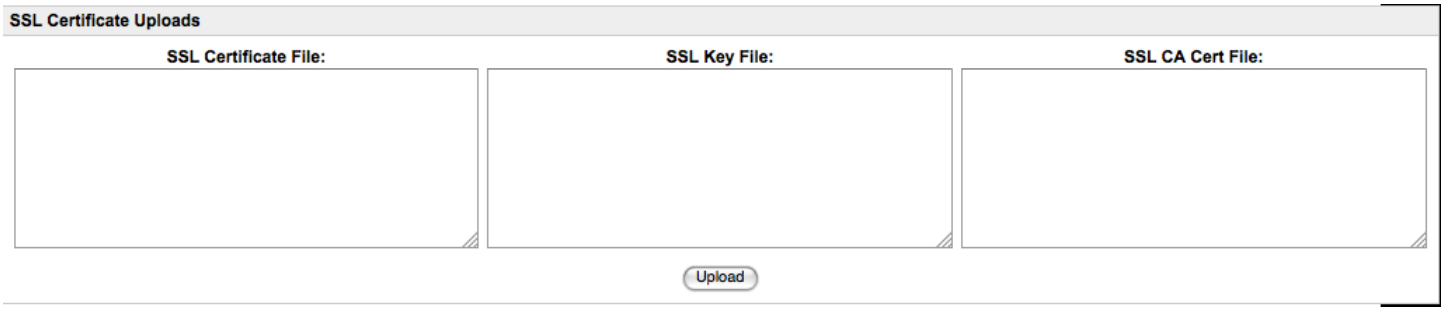
To generate a CSR, click the "*click here*" link by Certificate Generation Utility.

A new window will appear:

The Common Name will default to the hostname of your MailFoundry appliance. When you have completely entered the correct information, click Create CSR.

The *Download Files* link allows you to download the Private Key and CSR file that you generated previously under the SSL Certificate Generation section. You also can download the private Certificate Authority Root Certificate that was used to generate the initial certificates you are using now. If you download the private Certificate Authority Root Certificate and import it into your browser, you will no longer receive the warnings from your browser about an untrusted certificate.

SSL Certificate Uploads
The SSL Certificate Uploads section allows you to upload a new Certificate and Private Key file to use in place of the default ones generated when you enabled SSL support. If you try and mix the default generated cert/key with a private generated cert/key a failure will result and you will need to go to the console interface to reset your SSL settings. Also, you can upload a new Root Certificate to allow SSL Authentication to the interface.



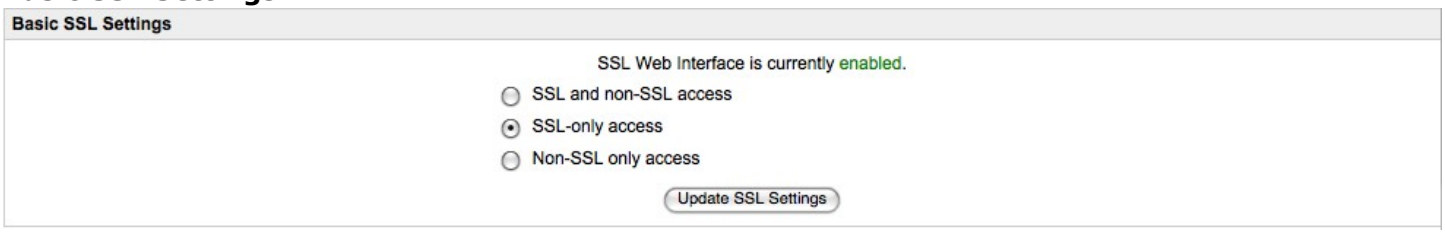
To upload the certificate, copy and paste it in the SSL Certificate File box.

If you need to upload a key file, paste it in the SSL Key File box.

If you need to upload an intermediate certificate file, paste it in the SSL CA Cert File box.

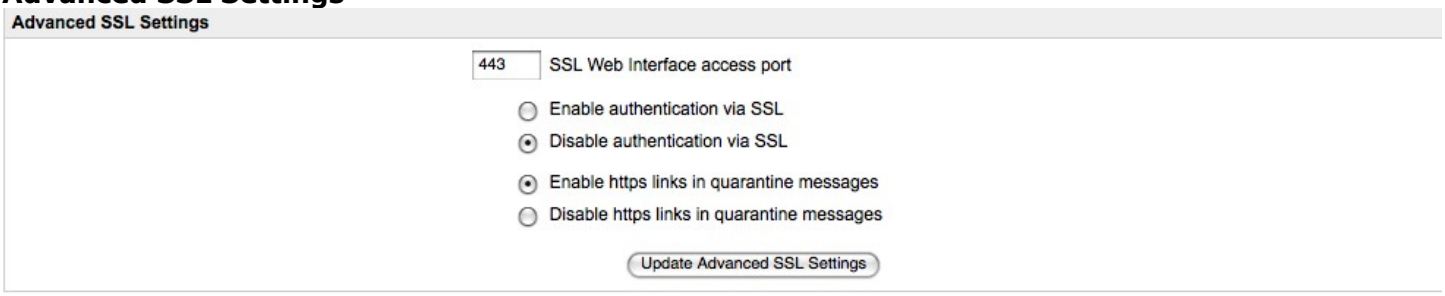
If you want to reset your SSL settings for any reason, go to the console interface to reset.

Basic SSL Settings



This is where you can enable SSL access for the admin interface, making that access either SSL only or SSL and non-SSL (HTTP and HTTPS).

Advanced SSL Settings


Advanced SSL Settings
443
SSL Web Interface access port
Enable authentication via SSL
Disable authentication via SSL
Enable https links in quarantine messages
Disable https links in quarantine messages
Update Advanced SSL Settings

Once you enable SSL access, you will now have access to the Advanced SSL settings. The Advanced settings allow you to change the port for SSL access to the admin interface, enable SSL authentication to the admin interface, enable SSL for SMTP, and choose HTTP or HTTPS links for quarantine messages.

If you are planning on using SSL authentication, you ***MUST*** first upload a new Certificate Authority Root Cert (see SSL Certificates tab to the left). If the Certificate Authority Root Cert is not uploaded first, you will be locked out of the admin interface. If this occurs, go to the console interface to reset your SSL settings for the admin interface.

SSL ***MUST*** be enabled to view the Advanced SSL Settings.

If you want to reset your SSL settings for any reason, go to the console interface / Setup Menu to reset.

Shutdown / Restart

In this section, you have two options. The first is to restart your MailFoundry appliance. This will stop all services, reboot the appliance and restart all services.

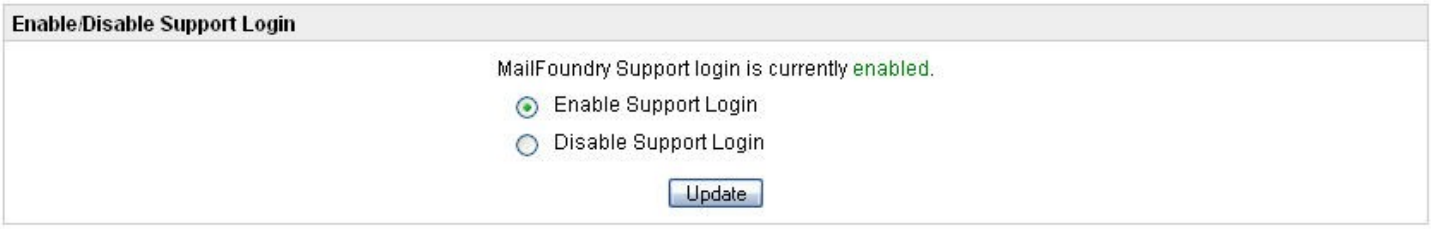
The second option is to shutdown your MailFoundry appliance. This will stop all services and power down the appliance.

If you choose to Shutdown the MailFoundry, you will see a dialog box prompting you to confirm that you want to shut down the appliance.

By default the option "Enable the repeating tone at shutdown state" will produce a loud repeating tone to be sounded until the unit has been unplugged from the power source when the appliance has fully completed its shutdown process.

It is recommended that you never power the appliance down using by pulling the plug from the power source or pulling the plug before the shutdown process has been completed as it could cause damage to the MailFoundry appliances system files.
Support Admin Login is used by MailFoundry technical support staff to remotely diagnose and repair system issues. Remote Login is done in a secure manner using SSH.

Support Admin Login

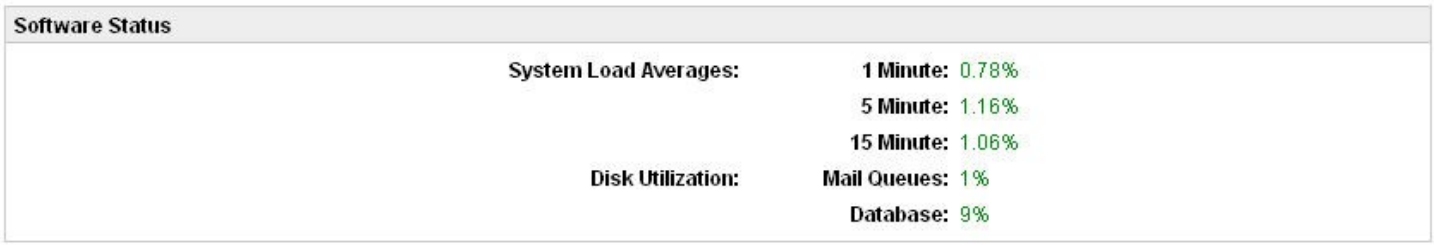


This option can remain disabled unless you are asked by a MailFoundry technical support staff member to enable it.

Once enabled, you will need to make sure that your network allows inbound and outbound connections to TCP/IP port 22 (SSH) from 66.18.18.11

Please note, that this setting is not preserved when your MailFoundry appliance is restarted. The default is disabled.

System Status



This section will display current real-time software and hardware utilization statistics including current and recent system load averages and disk utilization.

System Updates

System Update Methods
Manual System Updates
Automatic System Updates
Update Settings
NOTE: Switching from Manual to Automatic with pending updates available WILL automatically apply all of the updates currently pending.

Your MailFoundry appliance offers two methods for system updates, automatic or manual. The default is automatic updates.

System updates are often the release of new features and improvements. They do not include the updates for the anti-spam and anti-virus services. Those updates are always automatically delivered to the appliance.

Change Update Mode
To change the update mode from manual to automatic or reverse, click on the radio button next to the option you would like and click on the "Update Settings" button.

It is important to remember that if you switch from manual updates to automatic updates, and there are pending updates which have not been applied, all pending updates will automatically be applied to bring your appliance up-to-date.

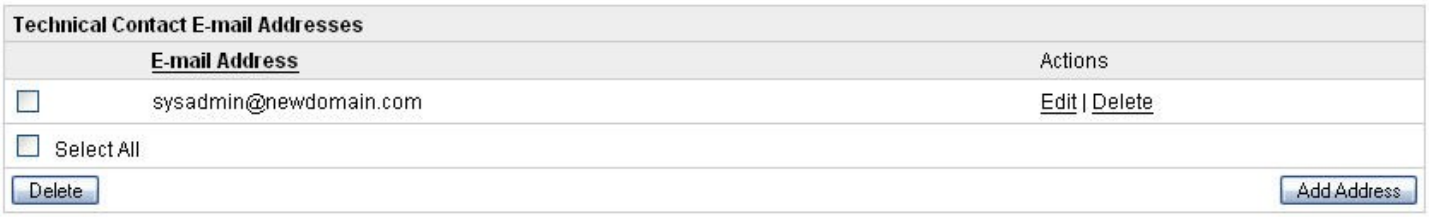
Managing Manual Updates

View Update Details
To view the release notes for a particular manual update, click on the "Details" link in the corresponding row.

Apply a Manual Update
To apply a manual update, click on the "Install Now" link next to the update you wish to apply. A confirmation screen will be displayed. Once your selection is confirmed, your MailFoundry appliance will begin the installation of the selected update.

If you choose to apply a manual update and there are previous updates which have not yet been applied, your MailFoundry appliance will install all previous updates automatically.

Technical Contact List



Addresses added to this list will receive notifications from the MailFoundry technical support staff such as new system update announcements. It is recommended that you have all system administrators added to this list.

Adding a New Address
To add a new entry to the Alert E-mail Addresses list, click on the "Add Address" button. Next, enter the full email of the user. Finally, click on the "Add" button.

Editing an Address
To edit an Address, click on the "edit" link in the corresponding row within the main listing.

Deleting an Address
To delete an address from the alert E-mail Address list, check the corresponding checkbox next to each listing you wish to delete. Next, click on the "Delete" button.

The Reports Tab

The System Settings tab provides the ability to customize emailed reports, view online statistics and manage your MailFoundry appliance's message queues.

Menu Structure	
Custom Emailed Reports	This option allows you to schedule and customize statistical emailed reports.
Emailed Report Addresses	This option allows you to define a list of email addresses who will receive customized statistical emailed reports.
Queue Status	This option allows you to view the Incoming, Outgoing, Un-scanned and Quarantine message queues.
Statistics	This option allows you to view detailed Statistics regarding your email traffic.

Custom Emailed Reports

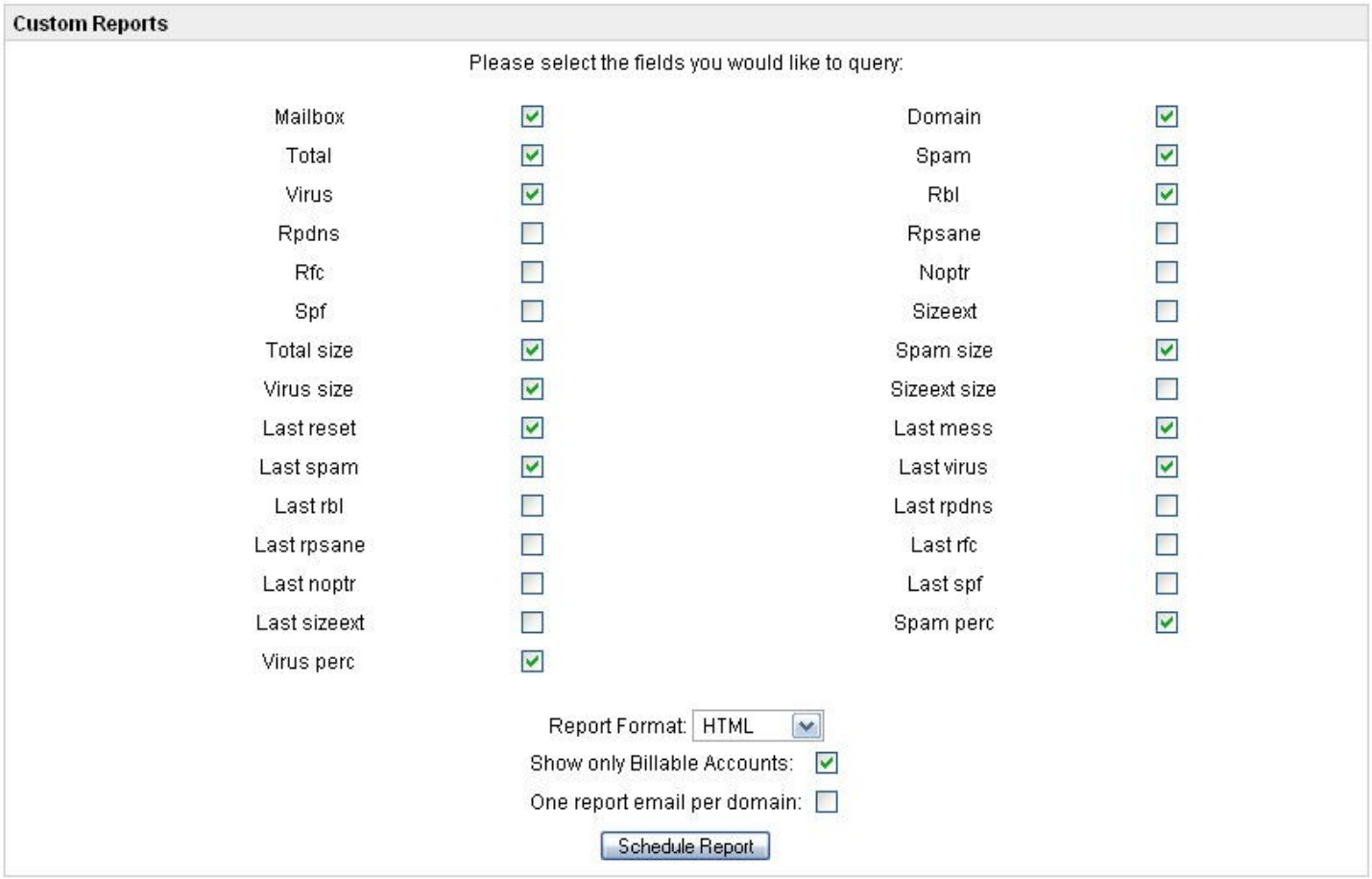
Custom emailed reports include information regarding your email traffic and scanning performance. Domain specific custom fields may also be included for identification purposes.

Report Scheduling

Custom Billing Reports Interval
Reports can be scheduled to run at any time to get a breakdown of the domain name, # of users and # of messages sent during a given month.
Your reports currently run on Daily at 0:00 AM.
Daily
Weekly
Monthly
at 12:00 AM
week runs from Sun - Sat
On day 1
Update

Custom emailed reports can be scheduled to be generated daily, weekly or monthly. For daily reports you can set the time at which the report will be generated each day (Example: 12:00 AM). For weekly reports you may define the period you would like covered (Example Sunday thru Saturday). For Monthly reports you can define which day of the month you would like the reports generated (Example: 1).

Customizing Reports



You can define which fields are included in the custom emailed reports such as the total number of mailboxes processed during the period. Place a checkbox next to each field you would like to include in your report.

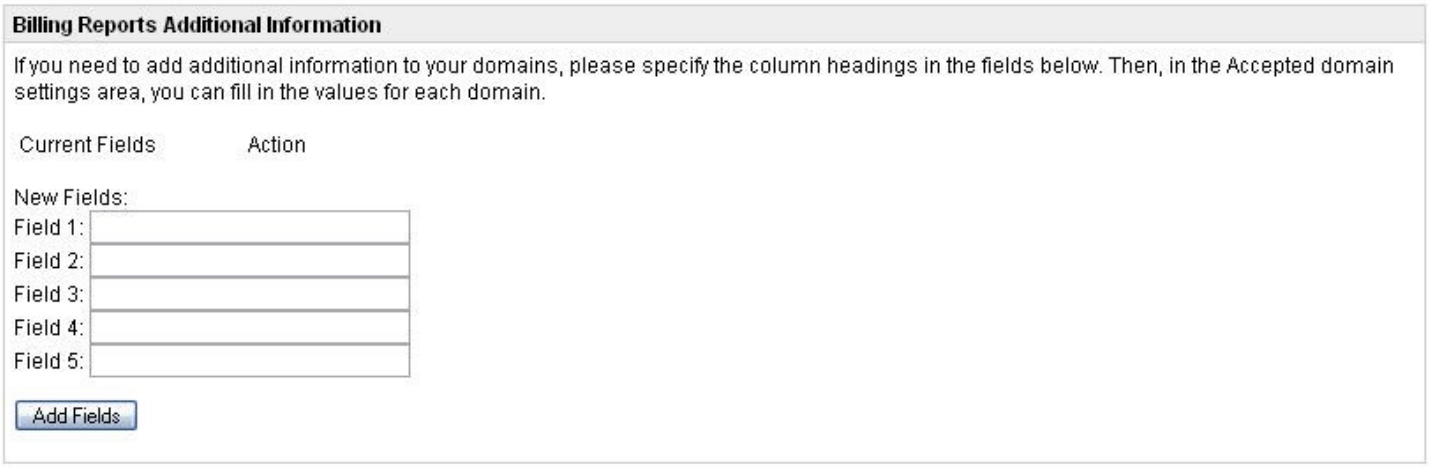
You can choose the report format, either text or HTML by changing the option listed in the "Report Format" drop down list.

You can use the "Show only Billable Accounts" to exclude any email accounts which are not considered "Billable" because of their placement in the Accepted Address system. This feature is typically useful for Internet Service Providers.

If you would like to have a separate email for each configured domain, check the "One report email per domain" option.

Once you have modified your settings, click on the "Schedule Report" button.

Adding Custom Fields

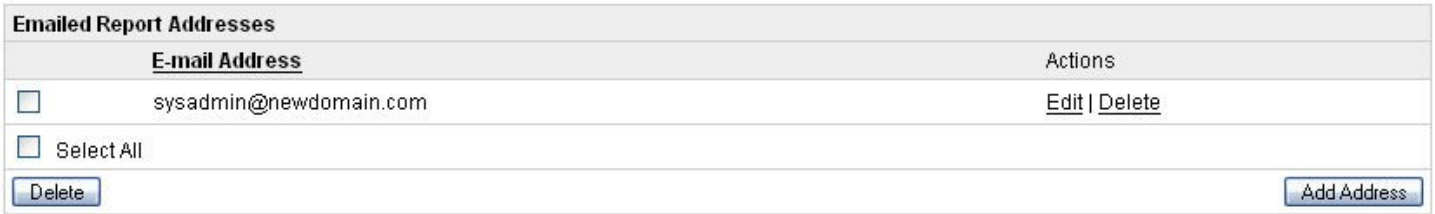

Billing Reports Additional Information
If you need to add additional information to your domains, please specify the column headings in the fields below. Then, in the Accepted domain settings area, you can fill in the values for each domain.
Current Fields
Action
New Fields:
Field 1:
Field 2:
Field 3:
Field 4:
Field 5:
Add Fields

You can use custom fields to further identify domains (For example: using an internal billing identification number).

To add a custom field, enter it in the "New Fields" section. Once completed, click on the "Add Field" button.

You will need to then edit each ofthe domains configured in your MailFoundry appliance to include the data for these new fields.

Emailed Report Addresses



If you are using the Custom Emailed Reports system, you will need to include a list of email addresses which will receive the reports.

Adding a New Address
To add a new entry to the list, click on the "Add Address" button. Next, enter the full email of the user. Finally, click on the "Add" button.

Editing an Address
To edit an Address, click on the "edit" link in the corresponding row within the main listing.

Deleting an Address
To delete an address from the list, check the corresponding checkbox next to each listing you wish to delete. Next, click on the "Delete" button.

Queue Status

Queue Status

Queue	Action	Total Count	Queue Processing Messages	
			Count	Failure Message
Incoming	View Reprocess All Delete All	5,371	5,287	hmdmx01.solinus.com[66.18.18.39] responded with failure: 451 Message failed
			42	Server hmdmx01.solinus.com[66.18.18.39] failed with: 452 Message exceeds quota limit for paydirtpen@gbpackersfan.com
			23	hmdmx01.solinus.com[66.18.18.39] responded with failure: 451 Invalid sender address
			13	Server hmdmx01.solinus.com[66.18.18.39] failed with: 452 Message exceeds quota limit for enosjr77@gbpackersfan.com
			3	Server hmdmx01.solinus.com[66.18.18.39] failed with: 452 Message exceeds quota limit for bpantzloff@gbpackersfan.com
			1	Server hmdmx01.solinus.com[66.18.18.39] failed with: 452 Message exceeds quota limit for lylebolen@gbpackersfan.com
			1	Server hmdmx01.solinus.com[66.18.18.39] failed with: 452 Message exceeds quota limit for pal18@gbpackersfan.com
			1	Unable to read SMTP greeting from hmdmx01.solinus.com[66.18.18.39]
Outgoing	View Reprocess All Delete All	613	15	Timed out while establishing SMTP connection with invites.movietickets.com[216.52.167.243]
			13	Timed out while reading SMTP greeting from eforward5.registrar-servers.com[50.30.32.27]
			10	Unable to establish SMTP connection with g01.MYINDIA41.COM[216.80.120.206]
			9	Timed out while establishing SMTP connection with smtpin.pinger.com[198.107.147.19]
			9	Timed out while establishing SMTP connection with am3a.NEWJOBSABROAD.COM[174.128.200.156]
			8	Unable to establish SMTP connection with mx1.dancekiss.info[204.27.57.230]
			8	Unable to establish SMTP connection with mx1.eatbuilding.info[204.27.57.230]
			8	Unable to establish SMTP connection with mx2.acceptbehavior.in[204.27.57.230]
			8	Unable to establish SMTP connection with mx2.complainfire.info[204.27.57.230]
			8	Unable to establish SMTP connection with mx2.coughdiscovery.info[204.27.57.230]
Unscanned	View Reprocess All Delete All	0	0	
Quarantine	View Release All Delete All	654,296	653,783	Junk
			513	Virus
			Last Updated: Wed, 31 Dec 1969 19:00:00 Click here to update stats	

Your MailFoundry appliance has a total of four queue systems. They are:

Incoming: Messages are stored in the incoming queue after they have been processed by the anti-spam, anti-virus and content filtering engines, but have not yet been delivered to the destination SMTP server.

Outgoing: Messages are stored in the outgoing queue when they are to be delivered to a destination SMTP server which is not on your network. These messages can be standard outgoing messages or messages being bounced back to the original sender due to a filtering action.

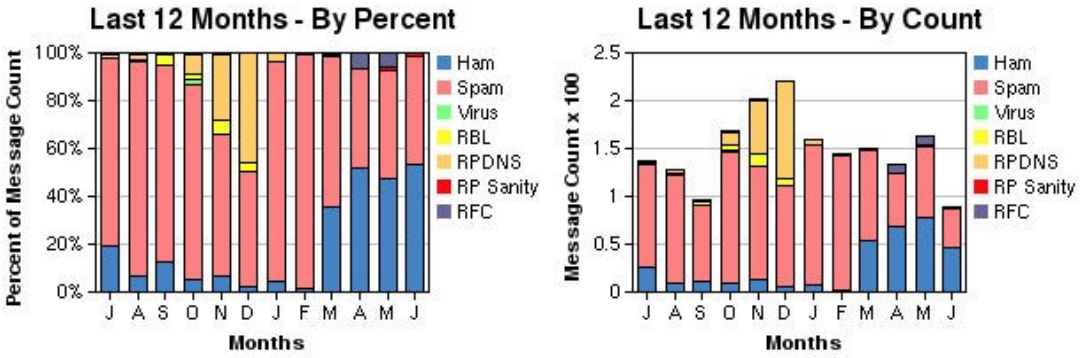
Unscanned: Messages are stored in the unscanned queue when they have not yet been processed by the anti-spam, anti-virus and content filtering engines.

Quarantine: Messages are stored in the quarantine queue after they have been identified as spam by the anti-spam engine, identified as a virus by the anti-virus engine or have been filtered by a content filter which is set to quarantine.

The queue status system gives you a detailed view of the current messages being processed or stored on your appliance. You will have the ability to search for messages within the queues as well as other management functions.

NOTE: To update statistics about all the queues, you will need to click the link that says Click here to update stats in the Quarantine Queue section. This may take some time to complete.

Statistics



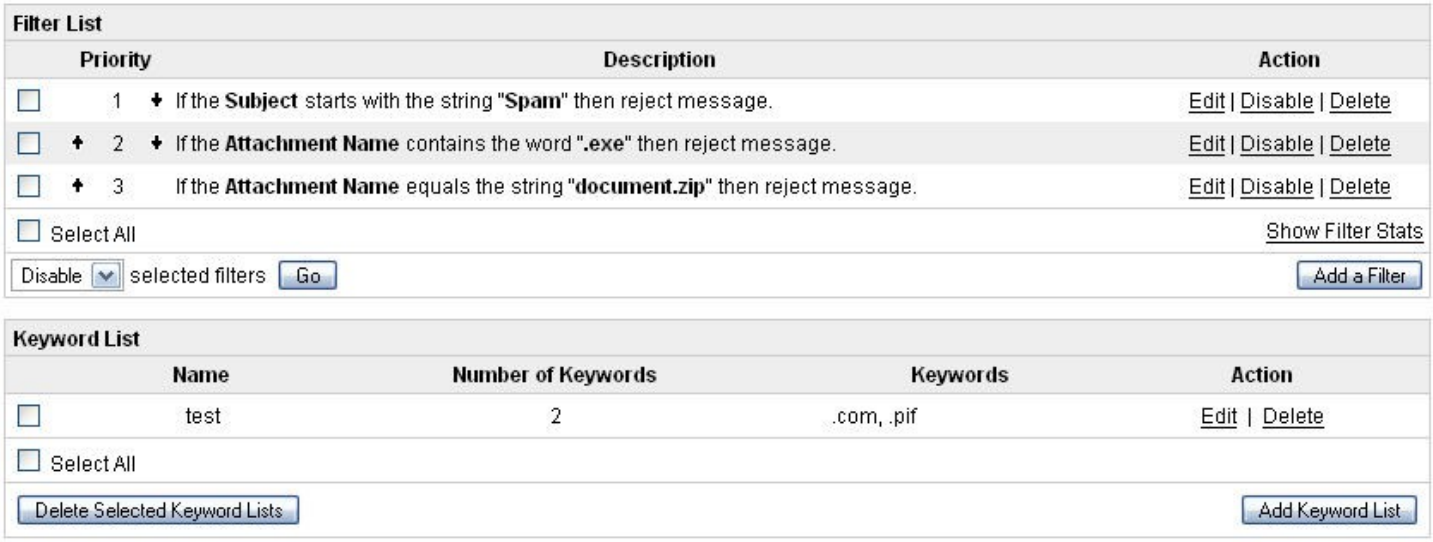
Breakdown by Month

Month	Domains	Total Messages	Allowed Messages	Allowed %	Blocked Messages	Blocked %	Actions
2004/07	2	137	26	18.98 %	111	81.02 %	Detailed Breakdown
2004/08	2	128	9	7.03 %	119	92.97 %	Detailed Breakdown
2004/09	3	96	12	12.50 %	84	87.50 %	Detailed Breakdown
2004/10	3	168	9	5.36 %	159	94.64 %	Detailed Breakdown
2004/11	4	201	13	6.47 %	188	93.53 %	Detailed Breakdown

Your MailFoundry appliance includes detailed message usage statistics including message volume details, filtering action details and more.

Statistics are collected in real-time and divided by month. A detailed break down of each month's statistics is provided.

Chapter 5: Custom Filters



Attachment Name: This option searches based on the file name of any attachments included with the message.

Entire Message: This option searches all possible portions of the message.

Any Header: This option searches all headers of the message.

Specific Header (Other): This option will search for the existence of a defined header in the message. To use this option, please the header name in the other text field (Example: X-Warning).

Chaining Filter Options

You can chain multiple filter options together to fine-tune the content you are searching for. To add multiple options, click on the "Chain" button in the upper right.

Filter Types

There are two types of filtering types which you can choose from. These types work in conjunctions with the "If" option. They are, "Does" and "Does Not". A "Does" type will trigger the filter when the "If" option is matched. The "Does Not" option will trigger the filter if the "If" option is not matched.

Filter "If" Option

There are several "If" options you can choose from for matching content within your filter. They include:

Starts with the string: This option will search for a particular string in the beginning of the message portion. This option is NOT case-sensitive.

Example, if you entered "Meeting", messages with the following content would trigger the filter:

"Meetings Scheduled Today"

The following content would NOT activate this filter:

"Scheduled Meetings Today" (Note: matching text is not at the beginning)

Starts with the exact string: This option will search for a particular string in the beginning of the message portion. This option IS case-sensitive.

Using the example from above, the following content would NOT trigger the filter:

"meetings Scheduled Today" (Note: case does not match)

Ends with the string: This option will search for a particular string in the end of the message portion. This option is NOT case-sensitive.

Example, if you entered "Meeting", messages with the following content would trigger the filter:

"We scheduled the meeting"

The following content would NOT activate this filter:

"Will you attend the meeting today" (Note: matching text is not at the end)

Ends with the exact string: This option will search for a particular string in the end of the message portion. This option IS case-sensitive.

Using the example from above, the following content would NOT trigger the filter:

"We scheduled the meeting" (Note: case does not match)

Equal the string: This option will search for a full text match in a message portion. This option is NOT case-sensitive.

Example, if you entered "Meeting Schedule", messages with the following content would trigger the filter:

"Meeting Schedule"

The following content would NOT activate this filter:

"Here is the Meeting Schedule" (Note: text is not a complete match)

Exactly equal the string: This option will search for a full text match in a message portion. This option IS case-sensitive.

Using the example from above, the following content would NOT trigger the filter:

"meeting schedule" (Note: case does not match)

Contain the word: This option will search for a word match in a message portion. This option is NOT case-sensitive.

Example, if you entered "Meeting", messages with the following content would trigger the filter:

"Meeting Schedule"

The following content would NOT activate this filter:

"Meetings Schedule" (Note: Meeting and Meetings are different words)

Contain the exact word: This option will search for a word match in a message portion. This option IS case-sensitive.

Using the example from above, the following content would NOT trigger the filter:

"meeting Schedule" (Note: case does not match)

Contain the string: This option will search for a string match in a message portion. This option is NOT case-sensitive.

Example, if you entered "Meeting", messages with the following content would trigger the filter:

"Meeting Schedule"
"Meetings Schedule"

The following content would NOT activate this filter:

"My Schedule" (Note: String not found)

Contain the exact sting: This option will search for a string match in a message portion. This option IS case-sensitive.

Using the example from above, the following content would NOT trigger the filter:

"meeting Schedule" (Note: case does not match)

"Then" Options

If a content filter is activated, it needs to trigger a "Then" option. "Then" options do the actual processing of a message. "Then" options include:

Quarantine message: This option will place the message into the quarantine system. If the recipient is configured to receive digest messages, they will see the filtered message listed. The message will not be delivered to the recipient unless they "Release" the message from the quarantine system.

Reject message: This option will reject the message sending an error to the sending SMTP server. It will not be delivered to the recipient.

Delete message: This option will accept the message from the sending SMTP server and then delete it. It will not be delivered to the recipient.

Redirect message to email address: This option will automatically forward the message to another email address. The original recipient will not receive a copy of the message.

Text page using email address: This option will send a shortened version of the message by SMTP to a text pager's email address. This option is often used with SMS enabled cell phones.

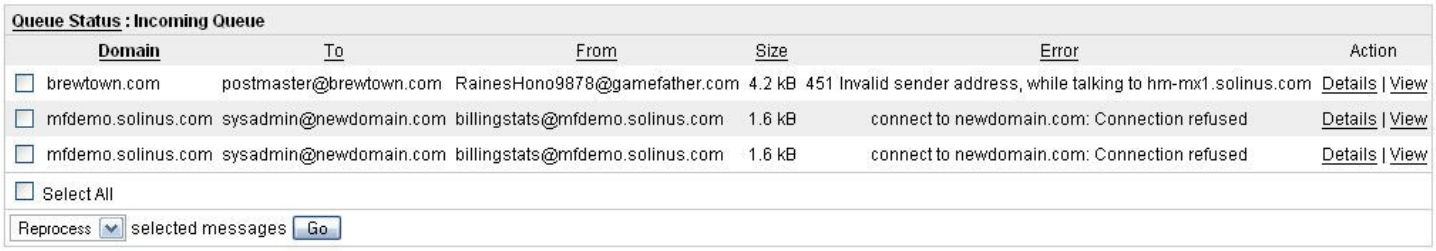
Filter Priority

The filter priority defines which filters are applied to the message in which order. Once a message matches a filter, no further filters matches will be detected.

Chapter 6: Queue Management

Your MailFoundry appliance provides you with many tools for managing messages which are stored within your appliance. These messages can be inbound messages which have not yet been delivered, outbound messages not yet delivered or messages which have been filtered and placed into the quarantine system.

Viewing a Queue



You may view a particular queue by clicking on the "view" link in the corresponding row.

Re-processing a Complete Queue

You can reprocess all messages stored in a particular queue by clicking on the "Reprocess All" link in the corresponding row.

Deleting all Messages from a Queue

You can delete all messages stored in a particular queue by clicking on the "Delete All" link in the corresponding row. This option will permanently delete the messages stored in the queue. You can not undelete the messages after this process.

View Message Details

To view the details of a particular message stored in a queue, click on the "Details" link in the corresponding row of the message listing.

Once you click on the "Details" link in the message list, a pop-up window will appear, providing you with details on the queued message. Information displayed includes the message to and from information, message size, time in queue, next process time and failure message.

Deleting a Message from the Queue
You can delete a message by clicking on the "Delete Message" link in the message detail window. You will be asked to confirm your selection before the message is permanently deleted.

Reprocess a Message
You can manually reprocess a message stored in the queue by clicking on the "Reprocess Message" link in the message detail windows. Your MailFoundry appliance will then attempt to complete delivery of the selected message.

Chapter 7: Frequently Asked Questions

Q: What type of spam detection does the MailFoundry appliance use?
A: MailFoundry uses the Solinus MessageIQ Engine to block spam. Based on human intelligence, the MessageIQ Engine uses a unique technology know as Spam Profiles, which are highly targeted to defend against specific spam attacks and spammers. By using this method, the MailFoundry network appliance offers an industry leading detection rate with an extremely low false positive rate.

Q: What percentage of spam is detected using the MailFoundry appliance?
A: In a majority of cases, spam detection rates range from 95% to 98% of total spam, with many of our customers experiencing a 99% detection rate.

Q: How accurate is the MailFoundry appliance?
A: MessageIQ, the anti-spam and anti-virus engine found in the MailFoundry network appliance, is designed to be the most accurate engine in the industry. By using human intelligence based, highly targeted Spam Profiles, we are able to keep false-positives to the extreme minimum. Most of our customers experience a false positive rate of less than one in one million messages.

Q: How can I be sure no legitimate e-mail is being deleted?
A: The MailFoundry network appliance gives you control over how detected spam messages are handled. The most commonly selected option is to use our advanced quarantine digest function which will allow users to view detected spam and release the message in the event it was incorrectly detected. You can also choose to redirect detected spam messages to another e-mail address, tag the message in the subject line or message header or you may delete the messages on the fly.

Q: Will MailFoundry detect and remove virus-infected e-mails?
A: Yes, MailFoundry will detect and remove all known viruses.

Q: How often are Spam Profiles updated?
A: New and updated Spam Profiles are automatically sent to the MailFoundry network appliance every five minutes.

Q: How often are virus definitions updated?
A: New and updated virus definitions are automatically sent to the MailFoundry Network appliance as new viruses are identified.

Q: What SMTP server products does the MailFoundry appliance work with?
A: The MailFoundry appliance will work with any server that supports the SMTP protocol. This includes Sendmail and Microsoft Exchange.

Q: Can I filter messages for multiple domains?
A: Yes, the MailFoundry network appliance supports multiple domains. Configurations may be system-wide or domain specific.

Q: Does the MailFoundry appliance work with multiple mail servers?
A: Yes, the MailFoundry network appliance can be configured to target any number of SMTP based mail servers. You may set routing globally or by domain.

Q: Can I use Real-time Black Lists (RBLs)?
A: You may choose to use RBL services in addition to the spam detection already offered by the MailFoundry appliance. RBL services are not activated by default.

Q: Can I add my own filters?
A: Yes, the MailFoundry appliance gives you the ability to define custom filters with many options. Filters can be system-wide, domain specific or address specific.

Q: Can I filter messages based on a keyword?
A: Yes, the MailFoundry appliance fully supports filtering by keyword. The ability to upload a keyword list is also provided.

Q: Does the MailFoundry appliance keep statistics related to my e-mail?
A: Yes, the MailFoundry appliance provides detailed statistics of your email traffic including the number of messages processed blocked as spam, blocked due to virus infection and several other blocking functions.

Q: Can I receive reports by email?
A: Yes, the MailFoundry appliance can send detailed reports to you by email on a scheduled basis.

Q: Will there be any delay in receiving email?
A: No, the MailFoundry appliance will process your e-mail quickly and send it to your target messaging server.

Technical Questions

Q: What hardware is the MailFoundry appliance based on?
A: The MailFoundry appliance is built using a custom-built Intel based 1U server.

Q: What operating system is the MailFoundry appliance based on?
A: The MailFoundry appliance is built using a secure, hardened version of the Linux operating system.

Q: What SMTP server is included inside the MailFoundry appliance?
A: The MailFoundry appliance includes hMail by Solinus, Inc. hMail is secured from worms designed to attack Sendmail, Microsoft Exchange and other 3rd party SMTP servers.

Q: Will I need to make changes to my DNS Settings?
A: Yes, all inbound MX records should point to the MailFoundry appliance. The MailFoundry appliance will route your inbound email to your messaging server.

Q: Can the MailFoundry appliance be placed behind a firewall?
A: The MailFoundry appliance is designed to be installed outside of your firewall. However, if you choose to install the appliance behind your firewall you must make sure that the following ports are open for inbound and outbound traffic. (22, 25, 110 and 443)

Q: Does the MailFoundry appliance support redundancy?
A: Yes, you can setup redundant or load balanced MailFoundry Appliances.

Q: What happens if my SMTP server is down?
A: If you SMTP server is down, the MailFoundry appliance will act as a storage device for your inbound mail. Once your SMTP server has retuned, mail will be forwarded.

Q: Can I place my SMTP servers address into my DNS Zone as a backup?
A: Placing an MX record for your SMTP server in your DNS zone will result in spam bypassing your MailFoundry appliance. Spammers will send to any MX record listed, regardless of the priority listed in the MX record. It is recommended that the only external MX record listed be protected by a MailFoundry appliance.

Chapter 8: Service and Technical Support

For technical support for your MailFoundry appliance, please use one of the following options.

Online Support: http://www.mailfoundry.com/support
Using our online support site, you can view our public knowledge base, submit support request and manage previously opened support requests.

Standard Telephone Support: +1-888-305-7776
Standard telephone support is available to all subscribers Monday through Friday, 8AM to 5PM central time (US).

Standard Email Support: support@mailfoundry.com
Standard email support is available to all subscribers. Support requests are answered during standard business hours of 8AM to 5PM central time (US).

24/7 Telephone Support: +1-888-305-7776
24/7 Telephone support is an additional option to subscribers. When calling after hours, you will need to provide your MailFoundry appliance serial number for verification of your 24/7 Telephone Support subscription.

If you have not subscribed to 24/7 support, please contact your Solinus account executive for details.